

Senate Standing Committee on Foreign Affairs, Defence and Trade

Inquiry into suicide by veterans and ex-service personnel – 6 February 2017

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: Whistleblower / Public Interest Disclosure

Question reference number: 2

Senator: Moore

Type of question: asked on Monday, 6 February 2017, Hansard page 26 Spoken

Date set by the committee for the return of answer: 24 February 2017

Question:

Senator MOORE: Is there a standard Defence document which explains whistleblower protection in Defence? If we can get a copy of that, that would be fine, because then we would know exactly what the personnel understand by 'whistleblower protection'.

Vice Adm. Griggs: We can give you the public interest disclosure material. I think that would be—

Answer:

In January 2014 in response to the introduction of the *Public Interest Disclosure Act 2013*, the Department of Defence renamed its Whistleblower Scheme to the Defence Public Interest Disclosure Scheme. To raise awareness of the *Public Interest Disclosure Act 2013*, the operation of the Defence Public Interest Disclosure Scheme and to advise on important aspects such as protections, Defence produced an administrative guide for personnel. A copy of the guide is at [Attachment A](#).

Additionally, Defence created a Defence Public Interest Disclosure Scheme website on both the internet and intranet. The Defence Public Interest Disclosure Scheme internet site is:

<http://www.defence.gov.au/afc/DisclosureScheme.asp>

Noting the Commonwealth Ombudsman's lead on the implementation and operation of the *Public Interest Disclosure Act 2013* across government, links from the Defence Public Interest Disclosure Scheme website to the Ombudsman's website is provided, where a wealth of information has been published to assist agencies and inform disclosers. The link to the Ombudsman's website is:

<http://www.ombudsman.gov.au/about/making-a-disclosure>

To complement this material, Defence has also released an online training course to further assist personnel in understanding the operation of the *Public Interest Disclosure Act 2013* in Defence. Finally, the Fraud Control and Investigations Branch, who manage the Defence Public Interest Disclosure Scheme, raise awareness of the *Public Interest Disclosure Act 2013* through face-to-face Fraud and Ethics presentations and other communication streams including the Defence Ethics Matters publication.

ASSISTANT SECRETARY FRAUD CONTROL
DEFENCE PUBLIC INTEREST DISCLOSURE SCHEME

Defence PID Scheme
ADMINISTRATIVE
GUIDE

Reviewed: 21 March 2016

PID hotline: 1800 673 502

PID email address: Defence.PID@defence.gov.au

Web Form – Report an Incident Form:

<https://dckrau004.dcb.defence.gov.au:60510/psp/dpdcrp3g/?cmd=logout>

CAVEAT

This Guide does not represent the entirety of the processes that are carried out under the authority of the *Public Interest Disclosure Act 1913* (PID Act).

The following text concentrates on:

- the actions of a public interest discloser who chooses to make a PID disclosure to an authorised recipient; and
- the subsequent actions of a Defence supervisor upon receiving a PID disclosure from a public interest discloser.

All other PID Act related processes (for example, the actions of an Authorised Officer upon receipt of a PID) are contained in reference material developed and maintained, within the office of the Assistant Secretary Fraud Control, as the responsible authority for PID matters in the Department of Defence.

For more comprehensive material relating to the administration of the PID Act, interested personnel can reference the Commonwealth Ombudsman's "*Agency Guide to the Public Interest Disclosure Act 2013*", which can be accessed at the Commonwealth Ombudsman's website www.ombudsman.gov.au/

Where this Guide states that an official or entity "must" do something, this reflects a matter of mandatory obligation under the *Public Interest Disclosure Act 2013*, with which the official or entity is required to comply.

OVERVIEW	4
What is the purpose of the PID Scheme Administrative Guide?	4
What is the purpose of the PID Act?	4
Defence PID Scheme	4
ROLES AND RESPONSIBILITIES.....	5
Public Officials	5
Principal Officer.....	5
Principal Officer's Delegate	5
Authorised Officer	5
Supervisors	6
HOW THE PID ACT WORKS	6
What is a public interest disclosure?	7
What is disclosable conduct?	7
What is not a disclosable conduct?	8
MAKING A PUBLIC INTEREST DISCLOSURE	8
How can a disclosure be made?	8
Who can receive a public interest disclosure?	9
What should a disclosure include?	9
What are the consequences of disclosing information anonymously?	9
Protection for disclosers	10
CONFIDENTIALITY	11
Will my information be kept confidential?	11
SUPPORT AND PROTECTION	11
Will I receive any support?	11
PROCEDURES FOR SUPERVISORS (INCLUDING COMMANDERS AND MANAGERS).....	11
What information should be given to an Authorised Officer?	13
Reporting PIDs through the chain of command or line management	13
ALLOCATING AND INVESTIGATING	14
What happens after a disclosure is made?	14
When will the Commonwealth Ombudsman investigate?	15
When should a risk assessment be undertaken?	15
What is a reprisal?	16
RESOURCES	18

DEFENCE PUBLIC INTEREST DISCLOSURE SCHEME

OVERVIEW

What is the purpose of the PID Scheme Administrative Guide?

1. The purpose of this Guide is to provide information about the operation of the PID Act within Defence to:

- Current and former Defence personnel, including contracted service providers; and
- Supervisors for dealing with disclosures of information made to them by their subordinates.

What is the purpose of the PID Act?

2. The *Public Interest Disclosure Act 2013* (PID Act) commenced on 15 January 2014. Defence has implemented the PID Act through the Defence Public Interest Disclosure Scheme (Defence PID Scheme).

3. The objectives of the PID Act are:

- To promote the integrity and accountability of the Commonwealth public sector;
- To encourage and facilitate the making of public interest disclosures (PID) by public officials;
- To ensure that public officials who make a PID are supported and are protected from adverse consequences relating to the disclosure; and
- To ensure that disclosures by public officials are properly investigated and appropriately dealt with.

Defence PID Scheme

4. The Department of Defence is an **Agency** under the PID Act. For the purposes of the PID Act, the Defence Material Organisation (DMO) is part of Defence.

5. The Australian Geospatial-Intelligence Organisation (AGO), the Australian Signals Directorate (ASD) and the Defence Intelligence Organisation (DIO) are separate Agencies under the PID Act. Public officials (including Defence personnel and contractors) working in any of these three intelligence agencies must consult the procedures developed within their own agency.

6. Defence has a range of robust and established systems for reporting and investigating complaints of suspected wrongdoing. These systems compliment the implementation of the PID Act within Defence. The PID Act recognises these pre-existing statutory based systems of investigating suspected wrongdoing and enables Defence to utilise these systems in dealing with PIDs. In that regard, while there is an additional PID reporting requirement on supervisors in Defence, the Defence PID Scheme has been developed to support supervisors in dealing with suspected

wrongdoing as soon as reasonably practicable and at the lowest possible command or management level using these existing systems.

7. For example, disclosures of information to supervisors in Defence that relate to unacceptable behaviour, fraud, or a criminal offence will still be dealt with through existing systems. However, supervisors now have an additional responsibility to give information about a disclosure to an Authorised Officer in the Office of the Assistant Secretary Fraud Control (ASFC) for PID assessment and reporting requirements.

ROLES AND RESPONSIBILITIES

Public Officials

8. In Defence, the term ‘Public official’ includes all current and former: Australian Defence Force members; Australian Public Servants; statutory office holders; contracted service providers and their subcontractors (in connection with entering into, or giving effect to, a Commonwealth contract).

9. All public officials **must** use their best endeavours to assist the Secretary (or delegate) in conducting an investigation under the PID Act.

10. All public officials **must** also use their best endeavours to assist the Commonwealth Ombudsman or the Inspector General of Intelligence Security (IGIS) in the performance of their functions under the PID Act.

Principal Officer

11. Under the PID Act, the Secretary of Defence is the Principal Officer who has a range of responsibilities, functions and powers under the PID Act. AGO, ASD and DIO have their own, separate, principal officers.

Principal Officer’s Delegate

12. The Secretary of Defence has, in writing, delegated all of the powers and functions under the PID Act to the ASFC, who is responsible for the management and operation of the Defence PID Scheme. This includes the development, promulgation, management, revision and maintenance of this guide and other material.

13. In this guide, the term ‘Principal Officer’ includes a Principal Officer’s delegate.

Authorised Officer

14. In addition to the Secretary and the ASFC, Authorised Officers have also been appointed in writing by the Secretary.

15. Authorised Officers are responsible for receiving disclosures, assessing whether they are PIDs and allocating PIDs to an agency.

16. For the purposes of the Defence PID Scheme all Authorised Officers are appointed within the Office of the ASFC. Authorised Officers can be contacted by any of the options outlined on the front of this Guide. A list of Authorised Officers can be found at <http://drnet.defence.gov.au/AssociateSecretary/AFCD/FCIB/Pages/Defence%20Public%20Interest%20Disclosure%20Scheme.aspx>

Supervisors

17. Supervisors, who are not appointed as Authorised Officers, have a mandatory reporting responsibility under the PID Act. In Defence, the term supervisor is taken to include commanders or managers, where the individual making the PID is in their chain of command or line management. Further information regarding this mandatory reporting obligation is contained in section titled Procedures for Supervisors (including commanders and managers) from paragraph 54 of this guide.

18. In this guide, where the word ‘supervisor’ is used it includes commanders and managers.

The Commonwealth Ombudsman and the Inspector General of Intelligence and Security

19. Both the Commonwealth Ombudsman and the Inspector General of Intelligence and Security (IGIS) have specific roles and functions under the PID Act. This guide will not cover these roles and functions; however, public officials should be aware that they may directly disclose information about suspected wrongdoing in Defence to an Authorised Officer in either of these Agencies.

HOW THE PID ACT WORKS

20. Broadly speaking, a PID is a disclosure of information, by a public official, that is:

- An Internal Disclosure: A disclosure within the Commonwealth public sector, to an Authorised public official in an Agency, concerning disclosable conduct; or
- An External Disclosure: A disclosure to anybody, if an internal disclosure of the information has not been adequately dealt with, and if wider disclosure satisfies public interest requirements; or
- An Emergency Disclosure: A disclosure to anybody if there is substantial and imminent danger to health or safety; or
- A Legal Practitioner Disclosure: A disclosure to an Australian legal practitioner for purposes connected with the above matters.

21. In general, most PIDs allocated to Defence will be Internal Disclosures. That is, a Defence public official will make a disclosure to their supervisor or to an Authorised Officer in Defence or another Agency.

22. Public officials in Defence should be aware that there are strict conditions set out in the PID Act for disclosing information as an External Disclosure, Emergency

Disclosure or Legal Practitioner Disclosure. If these conditions are not met, then the protections available to public officials under the PID Act may not apply.

What is a public interest disclosure?

23. A disclosure of information is a PID if:

- The disclosure is made by an individual (*the discloser*) who is, or has been, a public official; and
- The recipient of the information is the current supervisor of the discloser; or an Authorised Officer; and
- The information tends to show, or the discloser believes on reasonable grounds that the information tends to show, one or more instances of *disclosable conduct*.

24. Public officials may make a disclosure about suspected wrongdoing that occurred prior to the commencement of the PID Act and these disclosures will be actioned in accordance with the PID Act.

What is disclosable conduct?

25. Disclosable conduct is conduct of a kind mentioned in s29 of the PID Act that is conduct engaged in by: an Agency; a public official in connection his or her position as a public official; or a contracted service provider (or subcontractor) for a Commonwealth contract, in connection with entering into, or giving effect to, that Commonwealth contract.

26. The full definition of disclosable conduct is set out in section 29 of the PID Act.

27. In summary, disclosable conduct can include conduct that:

- Contravenes an Australian law
- In a foreign country, contravenes a foreign law that applies to the agency, official or service provider and corresponds to a law in force in the Australian Capital Territory
- 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, 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 property
- Unreasonably endangers health and safety of one or more persons
- Endangers the environment
- Is prescribed by any rules made under s.83 of the PID Act
- Involves abuse of the public official's position, or could, if proved, give reasonable grounds for disciplinary action against the public official

What is not a disclosable conduct?

28. Conduct is not disclosable conduct if it relates only to:

- disagreement with government policy, action or expenditure
- actions of Ministers, Speaker of House of Representatives and President of Senate
- conduct of Courts or Tribunals (unless administrative)
- proper activities of intelligence agencies

MAKING A PUBLIC INTEREST DISCLOSURE

Who can make a public interest disclosure?

29. Individuals wishing to make a public interest disclosure under the PID Act must be a public official. See paragraph 8 for the definition of public official.

30. A person who is not a public official can be 'taken to be' a public official, by an Authorised Officer. They can do this where they believe that an individual has information that concerns disclosable conduct and they have disclosed, or propose to disclose this to an Authorised Officer. This means that the Act has effect, and is taken to always to have had effect, in relation to the disclosure, as if the individual had been a public official when they obtained the information. See section 70 of the PID Act for more information.

How can a disclosure be made?

31. A disclosure can be made:

- Anonymously
- Orally or in writing
- Without the discloser asserting that the disclosure is made for the purposes of the PID Act (however, it will assist if the individual making the disclosure makes it clear the disclosure is made under the PID Act).

32. To gain the protections of the PID Act, a disclosure must be made in accordance with the Act - to a supervisor or an Authorised Officer. If an individual discloses information about suspected wrongdoing to another individual who is not authorised to receive it, **the disclosure will not be considered a PID and they will not be protected under the PID Act.**

33. An Authorised Officer can receive a disclosure by phone: 1800 673 502; email Defence.PID@defence.gov.au or completing an online report at: <http://intranet.defence.gov.au/afcd/sites/fcib/comweb.asp?page=43772&title=dws>

34. If a potential discloser wishes to make a disclosure about another Agency, the potential discloser should make that disclosure to the relevant agency or department. Further guidance can be sought from the Commonwealth Ombudsman's website:

www.ombudsman.gov.au or via the Agency's PID reporting procedures which should be available on the Agency's internet page.

Who can receive a public interest disclosure?

35. Generally, disclosures accepted under the Defence PID Scheme will be an Internal Disclosure. This means that the disclosure of information will be made by a public official to:

- their supervisor;
- a Defence Authorised Officer; or
- an Authorised Officer in an Agency to which the public official last belonged (where appropriate, these types of PIDs will be allocated by the other Agency to Defence to investigate).

36. If a potential discloser wishes to make a disclosure about another Agency, the potential discloser should make that disclosure to the relevant agency or department. Further guidance can be sought from the Commonwealth Ombudsman's website: www.ombudsman.gov.au or via the Agency's PID reporting procedures which should be available on the Agency's internet page.

37. Internal Disclosures can also be made by public officials in Defence directly to either the Commonwealth Ombudsman or IGIS (if security related) who may investigate the disclosure. However, where appropriate, these types of disclosures could be allocated to Defence for investigation.

38. The Commonwealth Ombudsman and the IGIS are Investigative Agencies under the PID Act and may investigate the disclosure under their own specific statutory powers.

What should a disclosure include?

39. A discloser or supervisor should prepare the following when preparing to disclose to an Authorised Officer:

- Clear and factual information
- Information that avoids speculation, personal attacks or emotive language
- Supporting evidence if it is available. However, it is critical that a discloser does not attempt to investigate the disclosure themselves to obtain evidence

What are the consequences of disclosing information anonymously?

40. Generally, a public official in Defence will identify themselves to their supervisor when disclosing information about suspected wrongdoing.

41. Public officials may choose to maintain their anonymity if the information is to be given by the supervisor to an Authorised Officer, or to the Principal Officer.

42. Where a public official discloses information directly to an Authorised Officer, they may also choose to maintain their anonymity.

43. However, there are reasons why disclosers should consider identifying themselves to an Authorised Officer or Principal Officer:

- The PID Act requires Defence to keep a discloser's identity confidential, subject to limited exceptions including the disclosers consent. The person's identity may nonetheless become apparent if an investigation is commenced.
- It is more difficult to ensure protection from reprisal if the department does not know the disclosers 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 the Authorised Officer cannot contact the discloser to seek necessary information, the matter may be prevented from proceeding.
- 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.
- 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.

44. An individual who has made an anonymous public interest disclosure may come forward at a later stage to disclose their identity and seek the protections of the PID Act.

45. If an individual wishes to make a disclosure about another Agency, the potential discloser should make that disclosure direct to the relevant Agency. Further guidance can be sought from the Commonwealth Ombudsman's website: www.ombudsman.gov.au or via the Agency's PID reporting procedures which should be available on the Agency's internet page.

Protection for disclosers

46. An individual is not subject to any civil, criminal or administrative liability for making a public interest disclosure.

47. It is an offence to take a reprisal, or to threaten to take a reprisal, against an individual because of a PID (including a proposed or a suspected PID). An offence against the PID Act can include reprisal action taken by a person against any other person, whether or not they actually made a PID.

48. The Federal Court or Federal Circuit Court may make orders for civil remedies (including compensation, injunctions and reinstatement of employment) if a reprisal is taken against a person because of a PID (including a proposed or suspected PID).

49. It is an offence for a public official who is involved in handling a disclosure to reveal the discloser's identifying information to anyone else without the discloser's consent or to use it for another purpose, unless it is for the purposes of the PID Act, an investigation by the Ombudsman or the IGIS, or another law of the Commonwealth or

prescribed law of a State or a Territory, or if the information has already lawfully been published.

50. Making a PID does not protect the discloser from liability for their own conduct. The protections under the PID Act do not apply to civil, criminal or administrative liability for knowingly making a false or misleading statement. However, it is important to realise that one of the objectives of the PID Act is to encourage and facilitate the making of PIDs. Unless there is strong evidence to show that an individual has made a false or misleading statement then civil, criminal or administrative action (including disciplinary action) should not be taken against the individual. It is strongly recommended that consultation should occur with the ASFC before such action is contemplated.

CONFIDENTIALITY

Will my information be kept confidential?

51. Under the PID Act, Defence (as with all agencies) is required to protect the discloser's identity. It is an offence for a public official who is involved in handling a disclosure to reveal the discloser's identifying information to anyone else without the discloser's consent or to use it for another purpose, unless it is for the purposes of:

- the PID Act;
- an investigation by the Ombudsman or the IGIS;
- an investigation under another law of the Commonwealth or prescribed law of a State or a Territory; or
- when the information has already lawfully been published.

SUPPORT AND PROTECTION

Will I receive any support?

52. An information pack will be made available to individuals who make a public interest disclosure. The pack will contain relevant information about the level of support available to disclosers in Defence noting the different needs of support people may require.

53. Similarly, an information pack will be made available to supervisors contacting the Defence PID Scheme about a discloser's information.

PROCEDURES FOR SUPERVISORS (INCLUDING COMMANDERS AND MANAGERS)

54. Supervisors play a key role in ensuring that Defence's workplace culture supports the making of a PID in a safe environment. Under the PID Act, supervisors are authorised to receive PIDs and have specific obligations to deal with disclosures.

55. When a Defence public official:

- discloses information about suspected wrongdoing to their supervisor; and
- the supervisor has reasonable grounds to believe that the information concerns, or could concern, one or more instances of disclosable conduct; then
- the supervisor **must**, as soon as reasonably practicable, give the information to an Authorised Officer in Defence.

56. Where there is uncertainty as to whether a disclosure is a PID, Defence encourages supervisors to act on the side of caution and give the information to an Authorised Officer.

57. While supervisors must comply with the PID reporting requirement, Defence expects supervisors to deal with matters reported to them in an expeditious manner and at the lowest possible command or management level. In this regard, supervisors who report disclosures by their staff to an Authorised Officer are not absolved of any other statutory or policy obligations (for example statutory obligations under the *Work Health and Safety Act 2011* and policy obligations under Defence Instructions (General) ADMIN 45-2: *Reporting and managing notifiable incidents*).

58. Defence's position on supervisors dealing with information disclosed to them by their staff is to:

- firstly, consistent with their responsibilities under other legislation and policy, deal with the information disclosed to them by their staff in a prompt manner and at the lowest possible command or management level; and
- secondly, give the information that was disclosed to them to an Authorised Officer as soon as reasonably practicable.

59. Defence's position on the operation of the Defence PID Scheme and the utilisation of separate agency responses to address PIDs at the first practicable opportunity has been endorsed by legal advice from the Australian Government Solicitor (AGS). In other words, there is no statutory restriction on supervisors utilising other mature Defence response mechanisms to resolve PIDs as long as the supervisor gives the information disclosed to them to an Authorised Officer, as soon as reasonably practicable.

60. Supervisors will therefore continue to maintain ownership of, and responsibility for addressing, any disclosure made to them by their staff through the Defence policy framework.

61. However, supervisors must understand that the PID Act protections that apply to a discloser remain in place even after the supervisor gives the information to an Authorised Officer. Supervisors must remember when dealing with these disclosures under another of Defence's response mechanism (for example, Code of Conduct, DFDA, Defence Inquiry), that the discloser must continue to be protected against any detriment and, where identity protection has been requested; the unlawful use or disclosure of their identifying information.

62. If the ASFC, as the Secretary's delegate, makes a determination to undertake a separate investigation under the PID Act in relation to any disclosure, a supervisor must use their best endeavours to assist in any investigation conducted.

63. Principal Officers, Authorised Officers and supervisors are not liable for any criminal or civil proceedings or any disciplinary action for any actions undertaken by them in good faith in the performance of a function or power under the PID Act.

What information should be given to an Authorised Officer?

64. Before giving information about a disclosure to an Authorised Officer, the supervisor should:

- take a written record of the facts of the disclosure; including the time and date of the disclosure,
- undertake an assessment of any risks that reprisal action might be taken against the discloser, and
- seek the discloser's consent to passing on their identifying information to other individuals for the purposes of investigating their disclosure.

65. When providing information to an Authorised Officer, supervisors should:

- give the Authorised Officer all records in relation to the disclosure (including any risk assessment information);
- if the person wishes to remain anonymous, advise the Authorised Officer;
- advise the Authorised Officer of any action being taken, or proposed to be taken to address the disclosure;
- inform the discloser that they have given the information to an Authorised Officer; and
- make appropriate records of the above.

66. Supervisors can give information about a disclosure to an Authorised Officer by phone: 1800 673 502; email Defence.PID@defence.gov.au or completing an online report at:

<http://drnet.defence.gov.au/AssociateSecretary/AFCD/FCIB/Pages/Defence%20Public%20Interest%20Disclosure%20Scheme.aspx>

Reporting PIDs through the chain of command or line management

67. Section 20 of the PID Act is an offence provisions relating to using or disclosing a discloser's identifying information. However, there are a number of statutory exceptions contained in this section of the PID Act.

68. Defence has received written legal advice from the AGS regarding the applicability of Defence instructions in relation to Commonwealth law. The AGS advised that Defence instructions of a mandatory nature (i.e. that impose mandatory obligations on Defence personnel) could be regarded as a 'law of the Commonwealth' for the purposes of the statutory exceptions under section 20(3) of the PID Act.

69. This means that a supervisor has statutory protection under the PID Act where they report identifying information about a discloser through the chain of command or line management in compliance with the mandatory content in a Defence instruction (or other statutory requirement). As best practice, supervisors should still seek the consent from the discloser before reporting this information.

70. Supervisors should only use or disclose identifying information about a discloser where there is a 'need to know' established by another 'law of the Commonwealth'. A discloser's identity should still be protected to the greatest extent possible.

ALLOCATING AND INVESTIGATING

What happens after a disclosure is made?

71. After an Authorised Officer receives a disclosure (either directly from a discloser or from a supervisor), they must use their best endeavours to decide within 14 days whether the disclosure must be allocated to an agency for investigation. The Authorised Officer must notify the discloser of the allocation decision.

72. An Authorised Officer may obtain information from such persons or make such inquiries as they think fit for the purpose of making this allocation decision.

73. If a disclosure is allocated to an agency (including Defence), the Principal Officer of the agency is required to investigate the disclosure. Where reasonably practicable, the Principal Officer will contact the discloser as soon as practicable after the disclosure is allocated to an agency.

74. A Principal Officer may consider conducting an investigation, outside of the provision of the PID Act. For example, a Principal Officer may determine it is more appropriate for a Code of Conduct investigation, a Defence Force Discipline Act (DFDA) investigation, a Defence Inquiry or some other investigative procedure established under a law of the Commonwealth to be undertaken, rather than an investigation under the PID Act.

75. In some instances, a Principal Officer will decide not to investigate the disclosure. There are specific statutory criteria under the PID Act that a Principal Officer must consider when deciding not to investigate a disclosure. However, the Principal Officer must advise the discloser of this decision, provide a reason for the decision and advise the discloser other available avenues for dealing with the matter.

76. There are mandatory obligations imposed on all agencies, including Defence for reporting to the Commonwealth Ombudsman about disclosures allocated to Defence, determinations not to investigate and investigation outcomes.

77. Once the disclosure is allocated to an agency the Principal Officer must complete the investigation within 90 days. There is provision for the Principal Officer to seek a time extension from the Commonwealth Ombudsman. If granted, the Commonwealth Ombudsman will notify the discloser of this time extension.

78. At the conclusion of the investigation, the Principal Officer must provide the discloser with a copy of the report of the investigation. Depending on the circumstances, some of the contents of the report may be redacted due to statutory, security, or intelligence reasons.

79. The Principal Officer must ensure that appropriate action is taken in response to any recommendations in a report of an investigation.

80. It is important to understand that, while a discloser may have a particular view on how they may wish their disclosure investigated, it is the Principal Officer that must make a decision on how the investigation will be conducted. Similarly, while a discloser reporting disclosable conduct may not wish the matter investigated, the Principal Officer may decide to undertake an investigation due to the significance of information disclosed.

81. On occasions, the investigative outcome may not accord with the expectations of the discloser. A discloser may discuss this issue with the Principal Officer and/or may discuss this issue with the Commonwealth Ombudsman.

82. An individual who has made a disclosure under the PID Act should not discuss the details of their disclosure with anyone, other than their supervisor (if reported to them), an Authorised Officer or a Principal Officer. Discussions with unauthorised individuals may compromise the protections that can be provided under the PID Act.

When will the Commonwealth Ombudsman investigate?

83. The Commonwealth Ombudsman may decide to investigate an Internal Disclosure made directly to them by a discloser or allocated to them by another Agency.

84. The Commonwealth Ombudsman will consider if there are special reasons to conduct the investigation. If the Commonwealth 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.

When should a risk assessment be undertaken?

85. Under the PID Act, Defence procedures for managing public interest disclosures are required to include assessing risks that reprisals may be taken against a person who makes a public interest disclosure [s.59(1)(a)].

86. 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.

87. 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.

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

89. When a supervisor receives a disclosure, they should conduct an initial assessment of the matter reported and the particular circumstances of the discloser to identify any known risk factors relating to the potential for reprisal.

What is a reprisal?

90. The PID Act makes it an offence to take a reprisal, or threaten to take a reprisal, against a person because of a public interest disclosure (including a proposed or suspected public interest disclosure).

91. To fulfil the responsibilities of the principal officer, authorised officers must assess the risk of reprisal, to a public interest discloser. To assess the risk of reprisal, an authorised officer needs to understand:

The elements of the offence provision:

- What is a 'reprisal'
- What is 'detriment'
- What is not a reprisal

92. To be a reprisal a person must cause detriment to another person (by act or omission) and this is an offence under the PID Act if it is done because of a PID. Detriment includes (but is not limited to) disadvantage in the form of dismissal, injury in their employment, alteration to their position to their detriment or discrimination between that employee and other employees. Normal and appropriate management action is not a reprisal, nor is administrative action that is reasonable to protect the person from detriment.

93. These protections remain in effect indefinitely, even after action taken under the PID Act has concluded.

94. The Federal Court or Federal Circuit Court may make orders for civil remedies (including compensation, injunctions and reinstatement of employment) if a reprisal is taken against a person because of a public interest disclosure (including a proposed or a suspected public interest disclosure)

95. For further information, the table below provides indicators for risks of reprisal or workplace conflict:

Threats or past experience	<ul style="list-style-type: none"> • Has a specific threat against the discloser been received? • Is there a history of conflict between the discloser and the subject of the disclosure, management, supervisors or colleagues? • Is there a history of reprisals? • Is it likely the disclosure will exacerbate this?
Confidentiality unlikely to be maintained	<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? • Are there circumstances, such as the discloser's stress level, that will make it difficult for them to not discuss the matter with people in their workplace? • Who in the workplace knows the discloser's identity? • Will the discloser become identified or suspected when the existence or substance of the disclosure is made known or investigated? • Can the disclosure be investigated while maintaining confidentiality?
Significant reported wrongdoing	<ul style="list-style-type: none"> • Are there allegations about individuals in the disclosure? • Is there more than one wrongdoer involved in the matter? • Is the reported wrongdoing serious? • Is or was the reported wrongdoing occurring frequently? • Is the disclosure particularly sensitive or embarrassing for any subjects of the disclosure, senior management, the agency or government? • Do these people have the intent to take reprisals – for example, because they have a lot to lose? • Do these people have the opportunity to take reprisals – for example because they have power over the discloser?
Vulnerable discloser	<ul style="list-style-type: none"> • Is or was the reported wrong doing

	<p>directed at the discloser?</p> <ul style="list-style-type: none"> • Are there multiple subjects of the disclosure? • Is the discloser isolated due to geographical location? • Are the allegations unlikely to be substantiated – for example because there is a lack of evidence? • Is the disclosure being investigated outside Defence?
--	---

RESOURCES

96. For more information relating to the Public Interest Disclosure Act, PID rules and PID standards made by the Ombudsman are at www.comlaw.gov.au

97. For information about the role and functions of the IGIS, see www.igis.gov.au

98. For information about breaches of the APS Code of Conduct, see www.apsc.gov.au

99. More information on the PID scheme, including fact sheets and guides, is on the Commonwealth Ombudsman's website at www.ombudsman.gov.au

100. A list of Frequently Asked Questions relating to the Public Interest Disclosure Act can be found on the Commonwealth Ombudsman's website at www.ombudsman.gov.au

101. For further information or feedback on this guide, please contact Acting Director – Fraud Control, Mr Steve Burge, by email: steven.burge1@defence.gov.au or phone (02) 6266 4162