

30 SEP 2016

VCDF/IN/2016/618

BRIEF FOR ASSOCIATE SECRETARY AND VICE CHIEF OF THE DEFENCE FORCE: APPROVAL TO PUBLISH INTERIM DEFENCE INSTRUCTION ADMIN 45-2 – INCIDENT REPORTING AND MANAGEMENT AND THE SUPPORTING INCIDENT REPORTING AND MANAGEMENT MANUAL

Division: Governance and Reform

Reference: FASGR/OUT/2016/

ASSOC SEC Reference:


Due Date: 28 September 2016

Recommendations

That you:

- (a) **Approve** publication of interim Defence Instruction ADMIN 45-2 – *Incident reporting and management* (interim Instruction) by using your delegation to issue Defence Instructions;
- (b) **Approve** publication of the *Incident reporting and management manual* (the Manual) under the current administrative policy arrangements;
- (c) **Note** that the publication of the interim Instruction and the Manual will cancel DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents* and DI(G) ADMIN 67-2 *Incident Recording*. The interim Instruction will remain extant for a period of 12 months from the date of its issue, at which point the relevant parts will be subsumed into a suitable permanent document.

Background

1. During March 2014, following the *Re-thinking Systems of Review and Investigation* initiative, the Chief of Service Committee endorsed structural and procedural changes relating to redress of grievance, investigation and inquiry. Flowing from that decision, the Inspector General of Defence (now the Assistant Secretary Audit and Fraud Control), was tasked to develop a consolidated incident reporting policy based on the current DI(G) ADMIN 45-2. Part of this task was to incorporate Defence obligations under the *Public Interest Disclosure Act 2013* into the consolidated incident reporting policy.
2.  s42
3. On 20 July 2015, the Secretary and Chief of the Defence Force issued Joint Directive 41/2015 to inform and direct responsibilities to implement changes to inquiry processes and incident recording in Defence.
4. The Joint Directive re-confirmed the task for the Inspector General of Defence to develop, sponsor and maintain a centralised incident reporting policy for Defence.

Key Issues

5. The Audit and Fraud Control Division has developed the attached draft interim Instruction and the Manual after significant and extensive consultation with key stakeholders across Defence. Where appropriate, feedback was incorporated into the documents to meet key stakeholder expectations.
6. The interim Instruction is a short-term policy document intended to:
 - (a) provide the legislative basis to require a Defence official to disclose or use identifying information in relation to a public interest disclosure, in accordance with a 'law of the Commonwealth' for the purposes of the *Public Interest Disclosure Act 2013*;
 - (b) impose obligations on Defence personnel regarding their responsibility to report incidents;
 - (c) impose obligations on commanders and managers regarding their responsibility to report, record and manage incidents; and
 - (d) impose and reinforce the mandatory requirement for commanders and managers to report more serious or complex incidents known as "notifiable incidents" to a Defence investigative authority.
7. I expect that, in the long term, the mandatory provisions articulated in the interim Instruction will be subsumed into Defence Instruction – *Administrative policy* once the new administrative policy framework is implemented. In the event that the new administrative policy framework is not implemented, I will seek your approval to re-issue the interim Instruction as a more enduring Defence Instruction.
8. Expanded guidance and advice on reporting, recording and management of incidents is provided in the supporting Manual.
9. There is currently no standardised and consistent workflow for managing reported incidents built into the Defence Policing and Security Management System. Some Groups and Services have worked with the policy sponsor to develop workflows, while others have very limited ability to manage incidents within the Defence Policing and Security Management System.
10. As part of the consultation, the policy sponsor requested that the Groups and Services provide the operating procedures they intended to use to manage incidents, so that appropriate workflows could be built into the Defence Policing and Security Management System. s47E
s47E
s47E As outlined in chapter 2, paragraph 2.15 of the Manual, once the Group and Service specific operating procedures are developed they will be incorporated into the published Manual as annexes.
11. Overall, the consultation process resulted in broad agreement over the content and intent of the interim Instruction and the Manual. Where differences of opinion existed, they were confined to issues of emphasis and process. Audit and Fraud Control Division considers the risk to Defence due to those differences to be extremely low.
12. Once the interim Instruction and the Manual are published, they will supersede the following policy documents, which will be cancelled:
 - a. DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents*; and
 - b. DI(G) ADMIN 67-2 *Incident recording*.
13. On 30 June 2016, Army approved DI(Army) ADMIN 23-2 *Management of reportable incidents* for publication. That was the last day on which Service Chiefs could issue new

single-Service Defence Instructions before the amended *Defence Act 1903* came into effect. New single-Service Defence Instructions cannot be issued from 1 July 2016 under the amended Act. Existing single-Service Defence Instructions will remain in force for 18 months following the commencement of the amended Act, at which time they will cease to have effect.

14. The Army policy is not consistent with the whole-of-Defence policy that has been developed with extensive consultation (including with Army). While provisions in a whole-of-Defence policy will take precedence over those in a single-Service policy, there is a risk that the reportable incidents within Army will not be managed in accordance with Defence policy. Audit and Fraud Control Division is working with Army Headquarters to determine what Army plans to do with its single-Service Defence Instruction.

Clearances

15. First Assistant Secretary Audit and Fraud Control, the sponsor of the interim Instruction and the Manual, has cleared both documents.
16. Extensive consultation with key stakeholder Groups and Services, including Defence People Group, Defence Legal Division and the Chief Finance Officer Group has been conducted and there are no remaining issues that could affect the implementation of this policy.

<p>s22</p> <p>Roxanne Kelley First Assistant Secretary Governance and Reform Tel: (02) 6265 6063 M: s22</p> <p>30 September 2016</p>	<p>(a) <u>Approved</u>/not approved (b) <u>Approved</u>/not approved (c) <u>Noted</u>/please discuss <i>see below</i></p> <p>s22</p> <p>Brendan Sargeant Associate Secretary</p> <p>4 October 2016</p>	<p>(a) <u>Approved</u>/not approved (b) <u>Approved</u>/not approved (c) <u>Noted</u>/please discuss <i>agree with below this doesn't make sense</i></p> <p>s22</p> <p>VADM R. J. Griggs VCDF</p> <p>17 October 2016</p>	
<p>Cleared/Approved by</p>	<p>Tony Corcoran</p>	<p>ASIMA</p>	<p>Tel (02) 6266 4080</p>
<p>Action Officer</p>	<p>Tony Brown</p>	<p>DAP</p>	<p>Tel (02) 6266 2720</p>

Attachments:

1. Draft interim Defence Instruction ADMIN 45-2 - *Incident reporting and management*.
2. Draft *Incident reporting and management manual*.

Roxanne

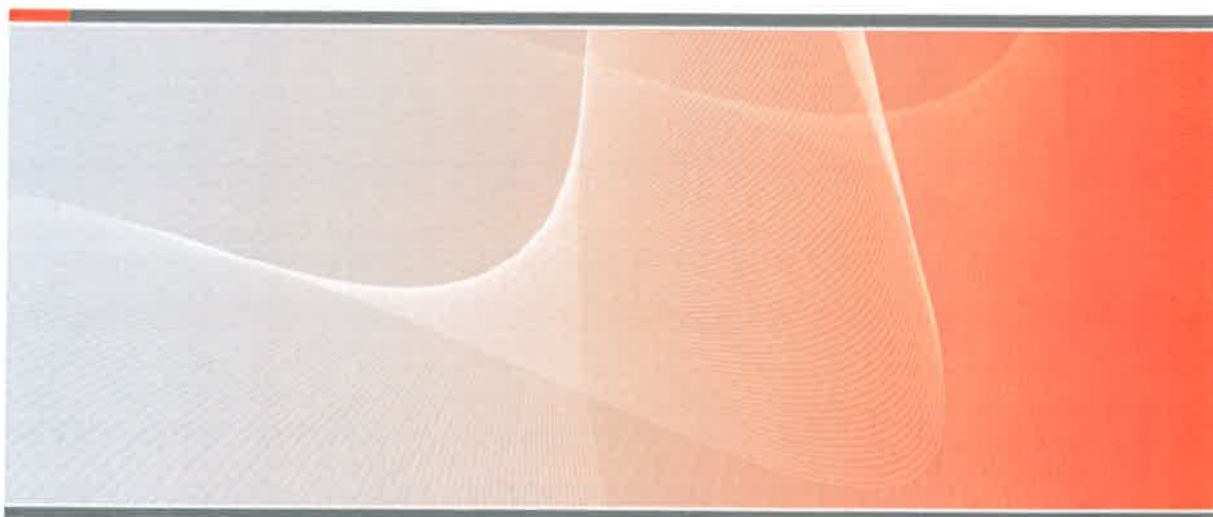
*How is Army different?
I assume that the implication of para 10 is that
in the future there will be a central/single responsibility
for all reported incidents. K & L*



Australian Government
Department of Defence

INTERIM DEFENCE INSTRUCTION ADMINISTRATION 45-2

INCIDENT REPORTING AND MANAGEMENT



<Signature block of the Associate
Secretary populated by DPS>

<Signature block of the Vice Chief of the
Defence Force populated by DPS>

[illegible]

INTERIM DEFENCE INSTRUCTION

INCIDENT REPORTING AND MANAGEMENT

Date issued: <Insert date approved for issue>

Issued by: Jointly by the Associate Secretary and the Vice Chief of the Defence Force in accordance with powers delegated to them by the Secretary of the Department of Defence and the Chief of the Defence Force under subsection 120A(3B) of the [Defence Act 1903](#). This interim Defence Instruction (interim Instruction) is issued under section 11 of the [Defence Act 1903](#).

Period of effect: <insert date 12 months from date of issue>

Purpose: This interim Instruction specifies the requirements that the Secretary and the Chief of the Defence Force have of all Defence personnel to report and manage incidents through either their line management or chain of command. For the purposes of the [Public Interest Disclosure Act 2013](#) this interim Instruction is a law of the Commonwealth.

Procedural material relating to this interim Instruction is contained in the [Incident reporting and management manual](#).

Management: This interim Instruction will remain extant for the duration of its period of effect at which point it will be cancelled. Within 12 months from its date of issue, the provisions to be retained will be subsumed into a suitable permanent document.

Availability: The latest version of this interim Instruction is available only from <http://intranet.defence.gov.au/home/documents/departme.htm>. Its currency cannot be guaranteed if sourced from other locations. It is available for public release.

Policy domain: Administration and governance domain

Accountable officer: Associate Secretary

Policy owner: First Assistant Secretary Audit and Fraud Control

Policy contact: Director Fraud Control

Cancellations: This interim Instruction cancels:

DI(G) ADMIN 45-2 – *The reporting and management of notifiable incidents*; and

DI(G) ADMIN 67-2 – *Incident recording*

Definitions: Definitions that apply to this interim Instruction are at Annex A.

INTRODUCTION

1. The manner in which managers and commanders manage incidents that impact on effectiveness and capability is fundamental to the success of Defence. These incidents may involve:
 - a. the well-being of Defence personnel;
 - b. infringement of legislative or regulatory requirements;
 - c. implications for safety and security;
 - d. potential to damage organisational reputation or brand; and/or
 - e. damage to equipment or facilities.

POLICY STATEMENT

2. Defence requires all incidents to be reported and managed through the Defence Australian Public Service line management or the Australian Defence Force chain of command and to be recorded in a central database in order to:
 - a. protect people, capability, operations and reputations;
 - b. ensure that accurate and contemporaneous records are made of the incident;
 - c. enable effective and timely responses to emerging issues;
 - d. ensure appropriate advice and specialist support is provided to managers and commanders from supporting agencies; and
 - e. facilitate strategic oversight by Defence leadership.

APPLICATION AND COMPLIANCE

3. This interim Instruction applies to all Defence personnel.
4. The terms of a relevant contract may extend the application of this interim Instruction to a contractor, consultant or outsourced service provider.
5. A mandatory requirement of this interim Instruction is identified through the use of the word **must**.
6. This interim Instruction comprises a 'general order' for the purposes of the [Defence Force Discipline Act 1982](#). Failure to comply with any mandatory or prohibitive requirement of this interim Instruction that applies to a Defence member may result in administrative or disciplinary action being taken against the Defence member.
7. This interim Instruction is a direction to Defence Australian Public Service employees for the purpose of subsection 13(5) of the [Public Service Act 1999](#)

(subsection 13(5) forms part of the Australian Public Service Code of Conduct). Failure to comply with a mandatory or prohibitive requirement of this interim Instruction that applies to a Defence Australian Public Service employee may result in investigation and possible sanctions as set out in section 15(1) of the [Public Service Act 1999](#), ranging from a reprimand to termination of employment.

8. Defence personnel who are authorised by the Secretary to execute contracts on behalf of the Commonwealth should consider whether there is a specific and documented reason to include in the terms of a contract the requirement for contractors, consultants and outsourced service providers to comply with the mandatory provisions of this interim Instruction and, if so, include such terms.

UNINTENDED CONSEQUENCES FROM APPLICATION OF THIS INTERIM INSTRUCTION

9. Where Defence personnel consider the application of this interim Instruction would produce an unintended or undesirable consequence, they should inform their supervisor about the issue to have the matter resolved with the policy owner.

10. In the event that this interim Instruction duplicates or is in conflict with material contained in another document intended for the internal administration of Defence, the mandatory provisions in this interim Instruction will prevail.

KEY ROLES, FUNCTIONS AND RESPONSIBILITIES

ALL DEFENCE PERSONNEL

11. Defence personnel who have reasonable suspicion that an incident has occurred, or who have received credible and/or believable information about any matter that might be categorised as an incident must, as soon as practicable but within 24 hours of commencement of duty, report the incident to their manager or commander. The following exceptions apply to this mandatory reporting obligation:

- a. the incident is a notifiable incident and is reported directly to a Defence investigative authority;
- b. a notifiable incident is reported directly to civilian police;
- c. a disclosure of information about an incident is made under the [Public Interest Disclosure Act 2013](#);
- d. an incident that might impact on a person's suitability to hold a security clearance is reported directly to the Australian Government Security Vetting Agency;
- e. a complaint of unacceptable behaviour is made to a respondent's manager; or
- f. a victim of physical violence or emotional trauma arising from the commission of a criminal act is not required to report the relevant incident under this interim Instruction, although Defence encourages them to do so.

12. An ADF Reservist who is not in uniform or not on duty and who reports an incident under this interim Instruction is deemed to be acting in the course of their official duty in making that report.

13. As a principle, Defence expects all Defence personnel, including reservists, whether engaged on duty or otherwise, to comply with the reporting requirements set out in this interim Instruction.

14. Subject to the requirements of Australian law, nothing in this interim Instruction is intended to override or affect potential legal privileges (including the privilege against self-incrimination) or confidences (including restricted disclosures made under DI(G) PERS 35-4 - *Reporting and management of sexual misconduct including sexual offences*) and disclosures of information made under the [Public Interest Disclosure Act 2013](#).

MANAGER AND COMMANDER RESPONSIBILITIES

15. Subject to statutory requirements, managers and commanders must, as soon as practicable but within 24 hours of commencement of duty, report all required information about a reported incident, through their line management or chain of command.

16. Managers and commanders must report any notifiable incident immediately to a Defence investigative authority. If there is doubt as to whether a matter is a notifiable incident, it is to be reported. Managers and commanders reporting a notifiable incident to a Defence investigative authority should note that this is a separate reporting action to the completion of a Defence incident record.

17. Completing other reporting requirements does not relieve managers and commanders of their reporting obligations under this interim Instruction except in accordance with the exceptions identified in paragraph 11.

18. Managers and commanders must manage any incident reported to them until all actions are complete or responsibility for managing the incident has passed to an appropriate internal or external investigative authority.

19. Managers and commanders must record details of the reporting and management of incidents in the authorised case management system using a Defence incident record.

20. Where access to the authorised case management system is unavailable, managers and commanders must make every effort to ensure a record, which contains all required information is created and a Defence incident record is completed, at the earliest opportunity.

HEAD DEFENCE INVESTIGATIVE AUTHORITY RESPONSIBILITIES

21. On receipt of a report of a notifiable incident, the head of a Defence investigative authority or authorised delegate must update any managers and commanders with responsibility for managing an incident on the progress of any assessment or investigation of the notifiable incident.

22. Managers and commanders must afford all reasonable assistance to personnel from the relevant Defence investigative authority in the execution of their duties to prevent any unreasonable impediment or interference with the investigation or inquiry process.

23. Managers and commanders must not direct or obstruct a Defence investigative authority in the execution of their duties.

MONITORING AND REPORTING

24. Managers and commanders are responsible for monitoring and reporting all reported incidents to the line management and chain of command. They must comply with integrity assurance reviews and audits into the application of this interim Instruction, conducted by the Associate Secretary.

POLICY IMPLEMENTATION

25. Group Heads and Service Chiefs are responsible for implementing this interim Instruction within their relevant Group/Service.

DEFINITIONS

Administrative policy. Is a term used to refer collectively to a class of documents that expresses the Defence senior leadership's approach to organising and managing the organisation. It consists of principles and rules that mandate requirements of, or provisions for, members of the organisation (what must be done) and procedures to assist in their implementation (how it should be done). Administrative policy is contained in different document types according to the intended purpose.

All required information. Is any information relating to an incident or notifiable incident that is required for recording purposes as prescribed in this interim Instruction or in the [Incident reporting and management manual](#).

Authorised case management system. Is any information technology enabled case management system authorised through this interim Instruction and/or the [Incident reporting and management manual](#).

Commander. Is an Australian Defence Force officer who, by virtue of a delegation or instrument of appointment, exercises authority and holds responsibility for assigned Defence personnel and includes an Administrative Commanding Officer.

Contractor. Is a person engaged by Defence under a contract that represents a business resource and is subject to direct management by Defence. Contractors would normally undertake Defence roles and are engaged as an alternative to normal Defence Australian Public Service employee resources. This would also apply in circumstances where the engagement of a firm is for labour hire involving specific personnel remunerated at hourly or daily rates. Defence members and Defence Australian Public Service employees are not included in this definition.

Consultant. Is a person or organisation engaged by Defence under a contract to undertake a consultancy that meets the following Department of Finance criteria for reporting on AusTender:

- a. the services to be provided involve the development of an intellectual output that assists with Defence decision making;
- b. the output will reflect the independent views of the consultant; and
- c. the output is the sole or majority element of the contract, in terms of relative value and importance.

Defence. Is the Department of Defence and the Australian Defence Force.

Defence Australian Public Service employee. Is a person employed under the [Public Service Act 1999](#) in the Department of Defence.

Defence civilian. As defined in section 3 of the [Defence Force Discipline Act 1982](#), is a person (other than a Defence member) who:

- a. with the authority of an authorised officer as defined in the [Defence Force Discipline Act 1982](#), accompanies a part of the Australian Defence Force that is outside Australia, or on operations against the enemy; and
- b. has consented, in writing, to subject themselves to Australian Defence Force discipline while so accompanying that part of the Australian Defence Force.

Defence locally engaged employee. Is any person engaged overseas by contract or under section 74 of the [Public Service Act 1999](#).

Defence member. As defined in the [Defence Force Discipline Act 1982](#) is a person who is:

- a. a member of the Permanent Navy, the Regular Army or the Permanent Air Force; or
- b. a member of the Reserves who:
 - (i) is rendering continuous full-time service; or
 - (ii) is on duty or in uniform.

Defence personnel. Are all Defence Australian Public Service employees, Defence members, Defence locally engaged employees, Defence civilians, and foreign personnel on exchange to Defence.

Defence premises. Means all land, buildings or other structures owned, occupied or used by Defence; and includes service land, ships, aircraft and vehicles as defined in section 3 of the [Defence Force Discipline Act 1982](#).

Disclosable conduct. Is defined in section 26 of the [Public Interest Disclosure Act 2013](#) and would include conduct for which disciplinary or administrative action might be taken.

Head Defence Investigative Authority. Means Director of Investigations and Recovery within the Fraud Control and Investigations Branch, the Provost Marshal – Australian Defence Force, the Service Police Provost Marshals of the Navy, Army and Air Force and the Director of Security Intelligence and Investigations within Defence Security and Vetting Service.

Incident. Is any non-routine event or occurrence that may have an effect on Defence, in particular capability, operations, personnel, security, safety, reputation, property, premises, environment, legal and ethical obligations, obligations to minors, and foreign relations. To avoid doubt, it includes all complaints made by Defence personnel, contractors, people involved in Australian Defence Force cadets, and members of the public, where the complaint is about Defence (including complaints about Defence personnel).

Manage. Means dealing with an incident in an effective and timely manner, exercising management and command responsibilities by fact-finding, problem solving and through transparent and accountable decision-making.

Manager. Means Defence personnel or contractors who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or perform the role of a first-

level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

Notifiable incident. Means any incident (as defined above) that:

- a. raises a reasonable suspicion that a criminal offence may have been committed under the criminal law of the Commonwealth, States or Territories, or the criminal law of another country;
- b. raises a reasonable suspicion that a serious offence has been committed under the [Defence Force Discipline Act 1982](#), not including incidents that are regarded as minor, which would ordinarily be dealt with by a Subordinate Summary Authority or under the Discipline Officer Scheme (noting that, if found to be more serious than initially determined, it may need to be reported as a notifiable incident);
- c. involves allegations of corrupt practices or behaviour, collusive tendering, conflict of interest or a lack of probity involving Commonwealth resources, including personnel, property or premises;
- d. is a suspected security incident (excluding minor security incidents), whether intentional, negligent or accidental, resulting in a failure to comply with a security requirement outlined in the [Defence security manual](#) or that may impact on a clearance holder's suitability to hold a security clearance;
- e. involves the death, serious injury (including self-harm) or disappearance of Defence personnel or the death, serious injury or disappearance of non-Defence personnel, involved in any Defence activity, or at any Defence property or premises (even where there may be no reasonable suspicion of an offence having been committed); or
- f. is an incident deemed by managers, supervisors or commanders to be serious, sensitive or urgent, not covered by the definitions above. That is, one that may bring Defence into disrepute; attract adverse media or parliamentary attention; or may adversely affect the efficiency of Defence, or impact on operational effectiveness or capability.

Outsourced service provider. Is a person or organisation engaged by Defence under a service contract to deliver a specified service or supply, usually against agreed milestones and deliverable requirements.

Period-of-effect. Is the period of time this interim Instruction remains extant.

Reasonable suspicion. Is where there is a suspicion, based on facts which, objectively seen by a reasonable person, is sufficient to give rise to a belief that an incident occurred. Reasonable suspicion is not the same as a belief that the person has committed an offence. If, upon looking at the material, there is a concern that an offence may have been committed, then a reasonable suspicion has been aroused.

Record. In the context of a manager's or commander's responsibility, means to input all required information about an incident into an approved form for use within an authorised case management system.

Report. In the context of all Defence personnel, means to report information about the details of an incident to: the chain of command; or if the incident is a notifiable incident to the chain of command or to a Defence investigative authority.

Security Incidents include:

- a. loss or theft or compromise of material classified CONFIDENTIAL and above, or significant quantities of material of a lower classification;
- b. loss, compromise, suspected or attempted compromise, theft or attempted theft, unauthorised access to, or use of classified equipment or information systems;
- c. loss or compromise of cryptographic keying material or Cryptographic Controlled Items;
- d. continuous or frequent minor security incidents involving the same person or work area where the combination of incidents indicates a disregard for security;
- e. inappropriate handling and storage of classified information;
- f. any actual loss, theft, attempted theft, recovery of, or suspicious incidents involving weapons, associated equipment (related to weapons) and explosive ordnance; and
- g. inappropriate handling, storage and transportation of weapons, associated equipment (involving weapons) and explosive ordnance.

Service Police. Means members of the Naval Police Coxswains, the Royal Australian Corps of Military Police and Air Force Police.

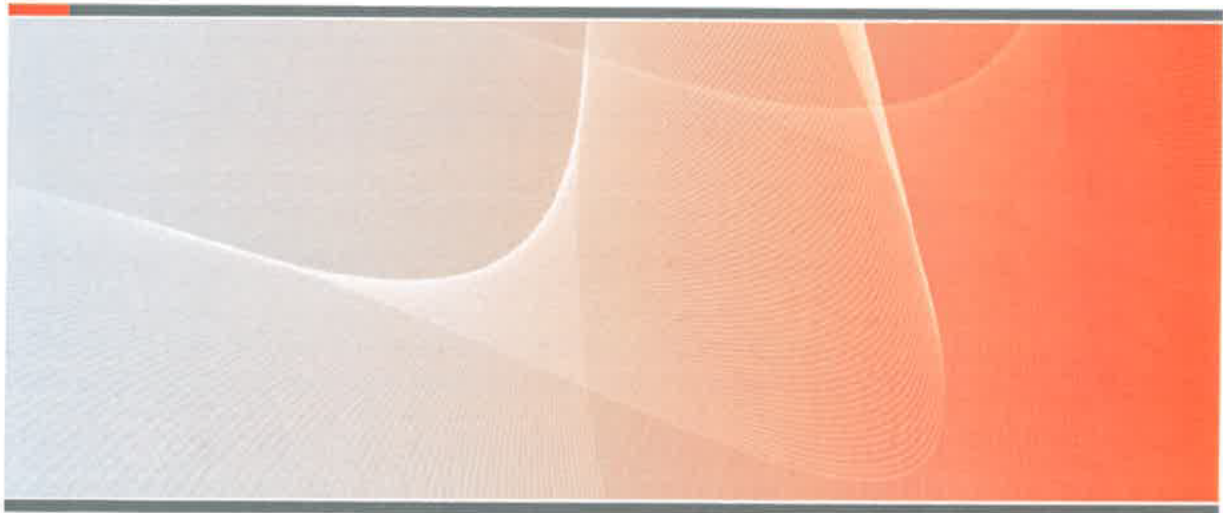
Supervisor. Means Defence personnel or contractors who have direct or line supervisory responsibilities for Defence personnel.



Australian Government
Department of Defence

INCIDENT REPORTING AND MANAGEMENT MANUAL

This manual refers to
interim Defence Instruction ADMIN 45-2 – *Incident reporting and management*



DPS to insert sig block of Assoc Sec
Name
Signature Position/Rank
Signature Title

Department of Defence
CANBERRA ACT 2600

Signature Date

DPS to insert sig block of VCDF
Signature Position/Rank
Signature Title

Department of Defence
CANBERRA ACT 2600

Signature Date

AMENDMENT CERTIFICATE

Amendment number	Chapter(s)	Amendment	Effected date

INCIDENT REPORTING AND MANAGEMENT MANUAL

Date Issued:	<insert date that the policy owner approved this issue>
Issued by:	The Associate Secretary and the Vice Chief of the Defence Force
Document management:	This manual will be reviewed five years from its date of issue or sooner if necessitated by business requirements and to ensure it continues to meet the intent of Defence's policy on this subject. Minor amendments may be made at quarterly intervals commencing three months after the date of issue.
Availability:	The latest version of this manual is only available from http://intranet.defence.gov.au/home/documents/data/DEFPUBS . Its currency cannot be guaranteed if sourced from other locations. It is available for public release.
Policy domain:	Administration and governance
Accountable officer:	Associate Secretary
Policy owner:	First Assistant Secretary Audit and Fraud Control
Policy contact:	Director Fraud Control
Purpose:	<p>This manual details policy and process changes to reporting, recording and managing incidents within Defence. These changes were initiated by the Re-thinking Systems of Review and Investigation process.</p> <p>The manual provides guidance to all Defence personnel on what constitutes an incident and how those incidents are to be reported. The manual also provides guidance to managers and commanders on recording and managing reported incidents to ensure an effective centralised incident recording system is maintained for accurate, efficient and timely reporting of incident within Defence and externally, where appropriate.</p>
Structure:	<p>Chapter 1 – Incident reporting by Defence personnel</p> <p>Chapter 2 – Incident recording by managers and commanders</p> <p>Chapter 3 – Reporting notifiable incidents</p>
Cancellation:	DI(G) ADMIN 45-2 – The reporting and management of notifiable incidents; and DI(G) ADMIN 67-2 – Incident reporting
Definitions:	Definitions that apply to this manual are at Annex 1A
Related documents:	Documents relating to this manual are listed at Annex 1B

Contents

Incident reporting by Defence personnel	1-1
Introduction	1-1
Scope and applicability of this manual	1-1
Requirement for Defence personnel to report an incident	1-2
Exceptions to reporting requirement	1-2
Reporting a notifiable incident directly to a Defence investigative authority	1-2
Reporting to civilian police services	1-2
Reporting a Public Interest Disclosure	1-3
Reporting security related incidents	1-3
Reporting suspected unacceptable behaviour	1-3
Victims of physical violence or emotional trauma	1-3
Annex 1A	1A-1
Definitions	1A-1
Annex 1B	1B-1
Related legislation and policy	1B-1
Incident recording by managers and commanders	2-1
Introduction	2-1
The Defence incident record	2-1
The Defence incident record process	2-2
Information required for completion of a Defence incident record	2-2
Submitting a Defence incident record	2-3
Recording Defence incident records in Defence Policing and Security Management System	2-3
Fact finding	2-3
Defence Policing and Security Management System privacy statement	2-4
Reporting Notifiable Incidents	3-1
Introduction	3-1
Notifiable incidents	3-1
Responsibilities of managers and commanders	3-1
Incidents involving persons under 18 years of age	3-1
How to report a notifiable incident	3-1
Actions on reporting a notifiable incident	3-2
Authority and role of Defence investigative authorities	3-2
Annex 3A	3A-1
Notifiable incident referral guide for departmental action	3A-1

CHAPTER 1

INCIDENT REPORTING BY DEFENCE PERSONNEL

INTRODUCTION

1.1 As defined at Annex 1A of this manual, an incident is any non-routine event or occurrence that may have an effect on Defence, in particular capability, operations, personnel, security, safety, reputation, property, premises, environment, legal and ethical obligations, obligations to minors, and foreign relations. To avoid doubt, it includes all complaints made by Defence personnel, contractors, people involved in Australian Defence Force cadets, and members of the public, where the complaint is about Defence (including complaints about Defence personnel).

SCOPE AND APPLICABILITY OF THIS MANUAL

1.2 This manual is an administrative policy framework document and applies to all Defence personnel.

1.3 The terms of a relevant contract may extend the application of any or all documents in the framework to a contractor, consultant or outsourced service provider.

1.4 The Secretary and the Chief of the Defence Force require Defence personnel to comply with provisions in manuals unless the particular circumstances warrant departure from the provisions.

1.5 Some manual provisions support Defence personnel to comply with obligations that exist in legislation, other applicable laws or in Defence Instructions. Defence personnel must not depart from manual provisions in a way that would result in a breach of applicable laws or Defence Instructions.

1.6 When considering a possible departure from a manual, the Secretary and the Chief of the Defence Force require Defence personnel to:

- a. consider whether a proposed departure from the provisions is reasonable and justified in the circumstances and will produce a better outcome for Defence;
- b. consult their supervisor, wherever practicable, about a proposed departure – a properly informed decision may involve consulting the policy owner; and
- c. be responsible and accountable for the consequences of departing from, or not adhering to, the content of a manual including where such departure or non-adherence results in a breach of applicable laws or leads to adverse outcomes for Defence.

1.7 Defence personnel may be subject to performance management, administrative action, or in some circumstances disciplinary action, where decisions or actions that depart from, or do not adhere to, manual provisions involve serious errors of judgement.

1.8 Failure to adhere to administrative policy may result in a breach of legislation or other legal requirement and sanctions under the legislation that may apply.

1.9 Defence personnel who are authorised by the Secretary to execute contracts on behalf of the Commonwealth should consider whether there is a specific and documented reason to include in the terms of a contract the requirement for

contractors, consultants and outsourced service providers to comply with the mandatory provisions of this manual and, if so, include such terms.

REQUIREMENT FOR DEFENCE PERSONNEL TO REPORT AN INCIDENT

1.10 All Defence personnel who have a reasonable suspicion that an incident has occurred, or who have received credible and/or believable information about any matter that might be categorised as an incident must, as soon as practicable but within 24 hours of commencement of duty, report the incident to their manager or commander.

EXCEPTIONS TO REPORTING REQUIREMENT

1.11 There are, however, a number of exceptions to this requirement. In this regard, Defence personnel who use any of the following methods to pass on information about an incident are considered to have met their obligations to report the incident.

REPORTING A NOTIFIABLE INCIDENT DIRECTLY TO A DEFENCE INVESTIGATIVE AUTHORITY

1.12 There will be circumstances where it is appropriate for Defence personnel to report a notifiable incident directly to a Defence investigative authority whether or not it is also reported to their manager or commander. For example:

- a. the notifiable incident is such that it requires the immediate attendance of service police; or
- b. there are compelling reasons why the notifiable incident should not be reported to a manager or commander (for example, the notifiable incident could involve the manager or commander of the person wishing to report the notifiable incident).

1.13 Defence expects that the Defence investigative authority will, where appropriate and as soon as reasonably practicable, consult with the affected Group or Service about the circumstances of the reported notifiable incident.

1.14 Comprehensive guidance on the reporting of notifiable incidents can be found at Chapter 3 of this manual.

REPORTING TO CIVILIAN POLICE SERVICES

1.15 In some circumstances, it may be appropriate for Defence personnel to report a notifiable incident directly to civilian police services.

Example

At a Defence establishment there are Service residences (married quarters) where concerns are held by an Australian Defence Force member and their family that the occupants of another Service residence nearby may be involved in domestic violence. The Australian Defence Force member believes, due to immediate concerns for the safety of individuals that an urgent response by civilian police is necessary. The Australian Defence Force member calls civilian police using the usual police emergency contact number.

1.16 Nothing in this manual is intended to prevent Defence personnel from reporting suspected criminal offences directly to civilian police services. Where a notifiable incident is reported to civilian police, and where consistent with the policy,

Defence also expects its personnel to report the notifiable incident to their manager or commander and/or a Defence investigative authority.

REPORTING A PUBLIC INTEREST DISCLOSURE

1.17 The [Public Interest Disclosure Act 2013](#) came into operation on 15 January 2014, providing a statutory framework for the disclosure of suspected wrongdoing and maladministration in the Commonwealth public sector.

1.18 Defence personnel making a disclosure under the [Public Interest Disclosure Act 2013](#) about suspected wrongdoing or maladministration within Defence are considered to have met any requirement to report an incident.

1.19 Defence has implemented the [Public Interest Disclosure Act 2013](#) through the operation of the [Defence Public Interest Disclosure Scheme](#). Further information and guidance on the operation of the [Public Interest Disclosure Act 2013](#) within Defence can be found at the [Defence Public Interest Disclosure Scheme](#) intranet website.

1.20 Additional material, fact sheets and guidance on the [Public Interest Disclosure Act 2013](#) can be found on the [Commonwealth Ombudsman's Public Interest Disclosure](#) website.

REPORTING SECURITY RELATED INCIDENTS

1.21 Guidance on reporting security related incidents can be found in [Part 2.12 of the Defence security manual](#).

1.22 Defence personnel reporting incidents in compliance with [Part 2.12 of the Defence security manual](#) are considered to have met their obligation to report an incident.

REPORTING SUSPECTED UNACCEPTABLE BEHAVIOUR

1.23 The Defence policy on reporting unacceptable behaviour is contained within [DI\(G\) PERS 35-3 - Management and reporting of unacceptable behaviour](#) and the [Complaints and alternative resolutions manual](#).

1.24 Defence personnel reporting unacceptable behaviour may report the complaint to the complainant's manager or to the respondent's manager. In either case, Defence personnel reporting incidents in this manner are considered to have met their obligations to report an incident.

VICTIMS OF PHYSICAL VIOLENCE OR EMOTIONAL TRAUMA

1.25 A victim of physical violence or emotional trauma arising from the commission of a criminal act is not required to report the incident in accordance with Defence policy, however, such victims are encouraged to report such incidents to their managers and commanders.

Annexes

1A Definitions

1B Related legislation and policy

ANNEX 1A

DEFINITIONS

All required information means any information relating to an incident or notifiable incident that is required for recording purposes as prescribed in [Interim Defence Instruction ADMIN 45-2 Incident reporting and management](#) and/or Annex 1B.

Authorised case management system means any information technology enabled case management system authorised through [Interim Defence Instruction ADMIN 45-2 Incident reporting and management](#) and/or Annex 1B.

Commander is an Australian Defence Force officer, who by virtue of a delegation or instrument of appointment exercises authority and holds responsibility for assigned Defence personnel and includes an administrative commanding officer.

Contractor is a person engaged by Defence under a contract that represents a business resource and is subject to direct management by Defence. Contractors would normally undertake Defence roles and are engaged as an alternative to normal Defence Australian Public Service employee resources. This would also apply in circumstances where the engagement of a firm is for labour hire involving specific personnel remunerated at hourly or daily rates. Defence members and Defence Australian Public Service employees are not included in this definition.

Consultant is a person or organisation engaged by Defence under a contract to undertake a consultancy that meets the following Department of Finance criteria for reporting on AusTender:

- a. the services to be provided involve the development of an intellectual output that assists with Defence decision making;
- b. the output will reflect the independent views of the consultant; and
- c. the output is the sole or majority element of the contract, in terms of relative value and importance.

Defence is the Department of Defence and the Australian Defence Force.

Defence Australian Public Service employee is a person employed under the [Public Service Act 1999](#) in the Department of Defence.

Defence investigative authority means the Directorate of Investigations and Recovery within the Fraud Control and Investigations Branch; the Australian Defence Force Investigative Service, the three service police organisations of the Navy, Army and Air Force that report to the provost marshal of each service; and the Directorate of Security Intelligence and Investigations within the Defence Security and Vetting Service.

Defence civilian as defined in section 3 of the [Defence Force Discipline Act 1982](#), is a person (other than a Defence member) who:

- a. with the authority of an authorised officer as defined in the [Defence Force Discipline Act 1982](#), accompanies a part of the Australian Defence Force that is outside Australia, or on operations against the enemy; and
- b. has consented, in writing, to subject themselves to Australian Defence Force discipline while so accompanying that part of the Australian Defence Force.

Defence locally engaged employee is any person engaged overseas by contract or under section 74 of the [Public Service Act 1999](#).

Defence member as defined in the [Defence Force Discipline Act 1982](#) is a person who is:

- a. a member of the Permanent Navy, the Regular Army or the Permanent Air Force; or
- b. a member of the Reserves who:
 - (1) is rendering continuous full-time service; or
 - (2) is on duty or in uniform.

Defence personnel is all Australian Public Service employees in the Department of Defence, Defence members, Defence locally engaged employees, Defence civilians, and foreign personnel on exchange to Defence.

Defence premises means all land, buildings or other structures owned, occupied or used by Defence; and includes service land, ships, aircraft and vehicles as defined in section 3 of the [Defence Force Discipline Act 1982](#).

Disclosable conduct is defined in section 26 of the [Public Interest Disclosure Act 2013](#) and would include conduct for which disciplinary or administrative action might be taken.

Head Defence Investigative Authority means the Director of Investigations and Recovery within the Fraud Control and Investigations Branch, the provost marshal of the Australian Defence Force, the service police provost marshals of the Navy, Army and Air Force and the Director of Security Intelligence and Investigations within the Defence Security and Vetting Service.

Incident is any non-routine event or occurrence that may have an effect on Defence, in particular capability, operations, personnel, security, safety, reputation, property, premises, environment, legal and ethical obligations, obligations to minors, and foreign relations. To avoid doubt, it includes all complaints made by Defence personnel, contractors, people involved in Australian Defence Force cadets, and members of the public, where the complaint is about Defence (including complaints about Defence personnel).

Manage means dealing with an incident in an effective and timely manner, exercising command and management responsibilities by fact-finding, problem solving and through transparent and accountable decision-making.

Manager means Defence personnel or contractors, who direct a range of human and physical resources and their associated financial responsibilities to achieve corporate objectives. A manager may be a first-level supervisor or performs the role of a first-level supervisor where they have immediate subordinates, as well as the role of a second-level supervisor where they have Defence personnel supervised by those subordinates.

Notifiable incident means any incident (as defined above) that:

- a. raises a reasonable suspicion that a criminal offence may have been committed under the criminal law of the Commonwealth, States or Territories, or the criminal law of another country;
- b. raises a reasonable suspicion that a serious offence has been committed under the [Defence Force Discipline Act 1982](#), not including incidents that are regarded as minor, which would ordinarily be dealt with by a subordinate summary authority or under the [Discipline officer scheme](#) (noting that, if

found to be more serious than initially determined, it may need to be reported as a notifiable incident);

- c. involves allegations of corrupt practices or behaviour, collusive tendering, conflict of interest or a lack of probity involving Commonwealth resources, including personnel, property or premises;
- d. is a suspected security incident (excluding minor security incidents), whether intentional, negligent or accidental, resulting in a failure to comply with a security requirement outlined in the [Defence security manual](#) or that may impact on a clearance holder's suitability to hold a security clearance;
- e. involves the death, serious injury (including self-harm) or disappearance of Defence personnel or the death, serious injury or disappearance of non-Defence personnel, involved in any Defence activity, or at any Defence property or premises (even where there may be no reasonable suspicion of an offence having been committed); or
- f. is an incident deemed by managers, commanders or supervisors to be serious, sensitive or urgent, not covered by the definitions above. That is, one that may bring Defence into disrepute; attract adverse media or parliamentary attention; or may adversely affect the efficiency of Defence, or impact on operational effectiveness or capability.

Outsourced service provider is a person or organisation engaged by Defence under a service contract to deliver a specified service or supply, usually against agreed milestones and deliverable requirements.

Period-of-effect is the period of time this interim Defence Instruction remains extant.

Reasonable suspicion is where there is a suspicion, based on facts which, objectively seen by a reasonable person, is sufficient to give rise to a belief that an incident occurred. Reasonable suspicion is not the same as a belief that the person has committed an offence. If, upon looking at the material there is a concern that an offence may have been committed, then a reasonable suspicion has been aroused.

Record in the context of a manager's or commander's responsibility, means to input all required information about an incident into an approved form for use within an authorised case management system.

Report In the context of all Defence personnel, means to report information about the details of an incident to: the chain of command; or if the incident is a notifiable incident to the chain of command or to a Defence investigative authority.

Security Incidents include:

- a. loss or theft or compromise of material classified CONFIDENTIAL and above, or significant quantities of material of a lower classification;
- b. loss, compromise, suspected or attempted compromise, theft or attempted theft, unauthorised access to, or use of classified equipment or information systems;
- c. loss or compromise of cryptographic keying material or cryptographic controlled items;
- d. continuous or frequent minor security incidents involving the same person or work area where the combination of incidents indicates a disregard for security;

- e. inappropriate handling and storage of classified information;
- f. any actual loss, theft, attempted theft, recovery of, or suspicious incidents involving weapons, associated equipment (related to weapons) and explosive ordnance; and
- g. inappropriate handling, storage and transportation of weapons, associated equipment (involving weapons) and explosive ordnance

Service Police means members of the Naval Police Coxswains, the Royal Australian Corps of Military Police and Air Force Police.

Supervisor means Defence personnel or contractors who have direct or line supervisory responsibilities for Defence personnel.

ANNEX 1B

RELATED LEGISLATION AND POLICY

[Crimes Act 1914](#)

[Criminal Code Act 1995](#)

[Defence Force Discipline Act 1982](#)

[Public Governance, Performance and Accountability Act 2013](#)

[Work Health and Safety Act 2011](#)

[Public Service Act 1999](#)

[Public Interest Disclosure Act 2013](#)

[Interim DI ADMIN 45-2 Incident reporting and management](#)

[DI\(G\) PERS 35-3 Management and reporting of unacceptable behaviour](#)

[DI\(G\) PERS 35-4 Reporting and management of sexual misconduct including sexual offences](#)

[DI\(G\) OPS 13-15 Incident scene initial action and preservation](#)

[Defence security manual \(eDSM\)](#)

[eDEOP 101 - Department of Defence Explosives Regulations, Regulation 1.3](#)

[DI\(A\) ADMIN 23-2 Management of reportable incidents](#)

[Accountable Authority Instruction 1- Managing risk and internal accountability](#)

[Defence aviation safety manual](#)

[Good decision making in Defence: A guide for decision-makers and those who brief them](#)

[Complaints and alternative resolutions manual](#)

[Form AE530 – Defence incident record](#)

[Records management policy manual](#)

[Defence casualty and bereavement support manual](#)

[Youth policy manual](#)

CHAPTER 2

INCIDENT RECORDING BY MANAGERS AND COMMANDERS

INTRODUCTION

2.1 The responsibility for recording a Defence incident report and reporting an incident (to line management, the chain of command or to a Defence investigative authority) are separate and distinct actions in this manual. Defence requires managers and commanders to:

- a. as soon practicable but within 24 hours of commencement of duty, report all required information about a reported incident, through their line management or chain of command;
- b. refer any notifiable incident to a Defence investigative authority in accordance with Chapter 3 of this manual; and
- c. record details of the reporting and management of incidents in the authorised case management system using a Defence incident record.

2.2 Defence is in the process of developing the Enterprise Recording Reporting and Case Management System. Until such time as this system is implemented, the authorised case management system for centralised incident recording in Defence is the Defence Policing and Security Management System.

THE DEFENCE INCIDENT RECORD

2.3 Managers and commanders should ensure all incidents reported to them are recorded in the Defence Policing and Security Management System either by using the link to the [Defence incident record](#) provided within the Defence Policing and Security Management System or by completing a [Form AE530 – Defence incident record](#) and uploading the details of that form into the Defence Policing and Security Management System by using the Defence incident record link.

2.4 Certain classes of incidents, however, have separate recording functionality within the Defence Policing and Security Management System. As such, managers and commanders do not need to complete a Defence incident record for the following types of incident:

- a. Security incidents independently reported under Part 2.12 of the [Defence security manual](#) which are recorded in the Defence Policing and Security Management System using forms [XP188](#) (security incident report) and [XP168](#) (contact report).
- b. Information disclosed by Defence personnel to their supervisors¹ under the [Public Interest Disclosure Act 2013](#), which is subsequently reported to an appointed public interest disclosure 'authorised officer' in Defence. This type of incident will be recorded independently in the Defence Policing and Security Management System through extant policy and

¹ Supervisors in Defence are encouraged to make themselves aware of their obligations under the Public Interest Disclosure Act. Supervisors can review the Public Interest Disclosure Act or access facts sheets and guidance on the Defence Public Interest Disclosure website or the Commonwealth Ombudsman's Public Interest Disclosure website.

processes. Further information on the procedures to be followed by commanders and managers on receipt of a public interest disclosure can be found in the [Defence Public Interest Disclosure Scheme Administrative Guide](#).

THE DEFENCE INCIDENT RECORD PROCESS

2.5 A Defence incident record is made as close as possible to the time of an incident, recording the circumstances of an incident as understood by the person making the record. A Defence incident record also records immediate management or command action taken or proposed in response to the incident.

2.6 Completion of a Defence incident record helps a manager or commander ensure they have assessed an incident based on the information available to them at the time. It is recognised that only a minimum of facts or information may be available at the time of completing a Defence incident record. Nevertheless, it provides a contemporaneous record that will support informed review and accountability for Defence in the management of incidents.

INFORMATION REQUIRED FOR COMPLETION OF A DEFENCE INCIDENT RECORD

2.7 The Defence incident record is intended to be a quick reference document, created in a consistent format that provides a reader with the following information (so far as it is readily available and able to be lawfully disclosed):

- a. brief details of what happened, including when, where, and who was involved (as understood by the person completing the Defence incident record at the time it is completed);
- b. the identity of the person in the unit/team responsible for managing the incident (and the person/property involved, usually the manager or commander of the unit/team involved);
- c. what actions were taken in the team/unit immediately following the incident;
- d. what further action is proposed, including in some cases that no further action is required;
- e. whether the incident has been or will be reported outside the team/unit involved; and
- f. reference to any files containing more detailed information about the incident.

2.8 The completion of a Defence incident record does not limit or replace the need, as required, for incidents to also be recorded as:

- a. a safety incident in Sentinel or on Form [AE 527](#) – Sentinel event report;
- b. a report of unacceptable behaviour using [ComTrack](#);
- c. an incident in the [Army Incident Management System](#);
- d. a notifiable incident with mandatory notifications requirements to a Defence investigative authority; or
- e. any other mandated reporting requirements necessary under legislation or extant policy.

SUBMITTING A DEFENCE INCIDENT RECORD

2.9 Defence requires all managers and commanders as soon practicable but within 24 hours of commencement of duty, to report all required information about a reported incident, through their line management or chain of command.

2.10 Where a Defence incident record or [Form AE530 – Defence incident record](#) is unavailable (for example because there is no access to the Defence Restricted Network), managers and commanders should use their discretion to determine the most appropriate format for recording an incident and as soon as reasonably practicable cause that information to be included in a Defence incident record in the Defence Policing and Security Management System.

2.11 Defence incident records are for documenting what was understood about an incident at the time, and documenting actions that were proposed or taken. Defence incident records are critical and auditable records that provide information about an incident and also enhance strategic visibility of incident management in Defence.

2.12 Managers and commanders should be aware that a Defence incident record may contain personal or sensitive information. All Defence incident records should include appropriate dissemination limiting markers, and should be handled and stored appropriately [see the [Privacy Act 1988](#), the [Defence privacy policy](#), the [Defence security manual](#) and the [Records management policy manual](#) for further information]. A Defence Policing and Security Management System Privacy statement is included in this manual at paragraph 2.19 of this chapter.

RECORDING DEFENCE INCIDENT RECORDS IN DEFENCE POLICING AND SECURITY MANAGEMENT SYSTEM

2.13 The Defence Policing and Security Management System provides for Defence incident records to be completed in three stages: initial; update and closure.

Initial: Provides the known facts of any incident on a who, what, where, and when basis.

Update: Records any developments regarding an incident including what, if any, further action is underway or is required. Where management of an incident is expected to be long term, a weekly/fortnightly/monthly update should be considered.

Closure: Provides information on how the incident was resolved to a point where no further action is necessary.

2.14 In some circumstances, a manager or commander may determine that no further action is required at the outset, in which case only an Initial Defence incident record need be completed.

2.15 While managers and commanders are responsible for ensuring all Defence incident record are recorded in the Defence Policing and Security Management System, Group Heads and Service Chiefs may choose to implement Group or Service specific standard operating procedures or protocols for incident record management.

2.16 Further guidance on the use and management of Defence incident records is available by accessing [Defence incident record instructions](#) within the [Audit and Fraud Control Division, Defence intranet website](#).

FACT FINDING

2.17 As a tool in determining the content of a Defence incident record (noting that an initial Defence incident record should not be delayed merely to collect additional information) or to decide whether an incident is a notifiable incident as described in Chapter 3 of this manual, managers and commanders may wish to conduct 'fact finding', which is a process of collecting information to support decision-making.

2.18 Guidance on the use of fact finding to assist decision making is available in the [Good decision-making in Defence](#) guide.

DEFENCE POLICING AND SECURITY MANAGEMENT SYSTEM PRIVACY STATEMENT

2.19 The information contained within the Defence Policing and Security Management System includes information of a personal nature, use and disclosure of which is governed by the [Privacy Act 1988](#), in particular Schedule 1 of the *Privacy Act 1988* (Section 14) – [Australian Privacy Principles \(APP\)](#). All users of the Defence Policing and Security Management System must ensure they are familiar with the [Australian Privacy Principles](#) which control the use and disclosure of personal information held by Defence.

2.20 Further references regarding privacy and limits on the use of Commonwealth and personal information include:

[Public Governance, Performance and Accountability Act 2013](#)

[Defence Force Discipline Act 1982](#)

[Public Service Act 1999](#)

[Crimes Act 1914](#)

[Criminal Code Act 1995](#)

CHAPTER 3

REPORTING NOTIFIABLE INCIDENTS

INTRODUCTION

3.1 Certain incidents involving Defence and its resources, including personnel, property and premises must be notified to the relevant Defence investigative authority so that appropriate action is taken. This chapter defines a notifiable incident and details the reporting procedures to be followed.

NOTIFIABLE INCIDENTS

3.2 A notifiable incident is any incident as defined in Annex 1A.

RESPONSIBILITIES OF MANAGERS AND COMMANDERS

3.3 Managers and commanders are required to determine whether an incident is a notifiable incident as soon as possible after becoming aware of the incident. Where it is determined that an incident is a notifiable incident, it should be reported immediately to a Defence investigative authority. If there is doubt as to whether a matter is a notifiable incident, it should still be reported to a Defence investigative authority. Advice may be sought from a Defence investigative authority or legal officer in appropriate cases. Legal and medical professional privilege may preclude the reporting of certain information.

3.4 Defence requires managers and commanders who have incidents reported to them (including notifiable incidents) to be aware of their statutory obligations under relevant legislation, regulations, Government and Defence policies.

3.5 In dealing with reported incidents including notifiable incidents, managers and commanders should refer to the [Notifiable incident referral guide for departmental action](#) to determine the most appropriate Defence investigative authority or support agency to which the incident should be referred.

3.6 In circumstances where the jurisdiction for investigating a notifiable incident is not clear, managers and commanders should report the notifiable incident to a Defence investigative authority. Defence expects that the head Defence investigative authority receiving the report will consider any jurisdictional issues and engage with other head Defence investigative authorities as appropriate.

INCIDENTS INVOLVING PERSONS UNDER 18 YEARS OF AGE

3.7 Guidance on dealing with matters involving persons under the age of 18 can be found in part 1 of the [Youth policy manual](#).

HOW TO REPORT A NOTIFIABLE INCIDENT

3.8 A report of a notifiable incident should be made by the most expeditious means possible in accordance with [Notifiable incident referral guide for departmental action](#). To ensure there is an auditable reporting trail, reports should be made in writing (for example by fax, email, message, mail or any other means appropriate to the circumstances). Where an urgent notifiable incident is reported by telephone or in person, a written report of the incident should be made at the earliest opportunity. Unit reporting of any matter should not be unduly delayed.

ACTIONS ON REPORTING A NOTIFIABLE INCIDENT

3.9 Managers and commanders will continue to manage incidents that are classified as a notifiable incident. Generally, the reporting of notifiable incidents to Defence investigative authorities will trigger a number of possible follow on actions that are intended to assist managers and commanders to manage a particular incident. The ability of Defence investigative authorities to pursue particular courses of action is directly related to their authority under law and policy.

3.10 Possible courses of action available to managers, commanders and Defence investigative authorities on receipt of a notifiable incident report are:

- a. managers and commanders ensure, wherever possible, action is undertaken to preserve and secure the incident scene in accordance with [DI\(G\) OPS 13-15 - Incident scene initial action and preservation](#) until arrival of police and investigative authorities.
- b. managers and commanders may be required by legislation or policy to report notifiable incidents to civilian authorities or other civilian investigative authorities. This may occur through a Defence investigative authority or directly to civilian authorities as necessitated by an extant emergency. In any event the appropriate Defence investigative authority must also be notified.

AUTHORITY AND ROLE OF DEFENCE INVESTIGATIVE AUTHORITIES

3.11 Defence investigative authorities conduct independent investigations into suspected notifiable incidents, or other matters as directed by the head Defence investigative authority, unfettered by the chain of command or line management. However, Defence investigative authorities are expected, where practicable, to consult closely with managers and commanders and exercise discretion around the proper conduct and integrity of any investigation. Impeding or interfering with a Defence investigative authority investigation may, depending on the circumstances, amount to a breach of the criminal law and/or Defence policy.

3.12 Managers and commanders are expected to take all reasonable steps to protect the integrity and confidentiality of an investigation. Information about suspicions, allegations, investigations or pending investigations are to be released only on a demonstrated need-to-know basis unless the Defence investigative authority conducting the investigation is satisfied that this will not adversely affect the conduct or integrity of the investigation.

3.13 Authority to suspend or cease an investigation is vested in the head of the relevant Australian Defence Force Defence investigative authority. In certain circumstances, however, where there are compelling reasons, the Chief of the Defence Force, the Vice Chief of the Defence Force, the Commander Joint Operations or a Service Chief may request that Provost Marshal – Australian Defence Force or the single-Service provost marshals (the relevant head Defence investigative authority), suspend an investigation.

3.14 A head Defence investigative authority may commence an investigation into any incident, reported or otherwise, relating to matters that fall within their respective jurisdiction. The Defence investigative authority retains sole authority over the conduct of an investigation and the investigation must not cease without the agreement of the relevant head Defence investigative authority.

3.15 A head Defence investigative authority may decide not to commence an investigation and refer the matter back to management or command for inquiry at unit level.

Annex

3A .Notifiable incident referral guide for departmental action

ANNEX 3A

NOTIFIABLE INCIDENT REFERRAL GUIDE FOR DEPARTMENTAL ACTION

Incident types	Incident description	Reported to	Relevant legislation and policy
1	Incidents that raise a reasonable suspicion that a civilian criminal offence has been committed where the incident involves Defence personnel, a Defence activity, property or premises (not including suspected <u>Defence Force Discipline Act 1982</u> offences reported below)	<p>Action: Commonwealth/state/territory civilian police organisations</p> <p>Contact: Phone: 000</p> <p>Australian Defence Force Investigative Service/service police</p> <p>Contact: adfishq.operations@defence.gov.au Phone: 1300 233 471</p> <p>Australian Defence Force Investigative Service operations duty mobile: s22</p> <p>Directorate of Investigations and Recovery – if fraud or corruption related</p> <p>Contact: fraud.investigations@defence.gov.au Phone: 02 6266 4322</p> <p>Defence Security and Vetting Service - if security related</p> <p>Contact: Security Incident Centre Phone: 02 6266 3331 After hours: s22 XP168 or XP188</p>	<p>Commonwealth Fraud Control Framework 2014</p> <p>Australian Government Investigations Standards 2011</p> <p>Defence Force Discipline Act 1982</p> <p>AAI 1.3.1.16 – Fraud control</p> <p>Interim DI ADMIN 45-2 Incident reporting and management</p> <p>Defence security manual</p> <p>DI(G) PERS 35-4 Reporting and management of sexual misconduct including sexual offences</p>

Incident types	Incident description	Reported to	Relevant legislation and policy
		Information: Line management/chain of command	
2	Incidents that raise a reasonable suspicion that a serious Defence Force Discipline Act 1982 offence has been committed	Action: Australian Defence Force Investigative Service/service police Directorate of Investigations and Recovery – if fraud or corruption related Defence Security and Vetting Service - if security related Information: Line management/chain of command	Defence Force Discipline Act 1982 AAI 1.3.1.16 – Fraud control Interim DI ADMIN 45-2 Incident reporting and management Defence security manual
3	Allegations of corrupt practices and behaviour, collusive tendering, lack of probity or conflict of interest issues involving Commonwealth resources, including personnel, property or premises	Action: Directorate of Investigations and Recovery Information: Line management/chain of command Australian Defence Force Investigative Service (if <i>Defence Force Discipline Act 1982</i> offence suspected)	Commonwealth Fraud Control Framework 2014 Australian Government Investigations Standards 2011 AAI 1.3.1.16 – Fraud control Interim DI ADMIN 45-2 Incident reporting and management
4	Suspected security incidents	Action: Defence Security and Vetting Service (Refer form XP188 – Security Incident Report) Information: Australian Defence Force Investigative Service (if Defence Force Discipline Act 1982 offence suspected)	Interim DI ADMIN 45-2 Incident reporting and management Defence security manual XP188 or XP168

Incident types	Incident description	Reported to	Relevant legislation and policy
5	Death/serious injury, including self-harm, or disappearance of Defence personnel, or death/serious injury involving any Defence activity, property or on Defence premises (excluding enemy combatants)	<p>Line management/chain of command</p> <p>Relevant provost marshal</p> <p>Action:</p> <p>Line management/chain of command</p> <p>Australian Defence Force Investigative Service/service police (secure scene on behalf of Directorate of Select Incident Review and/or Inspector General of the Australian Defence Force)</p> <p>Information:</p> <p>Relevant provost marshal (if suspected Defence Force Discipline Act 1982 offence or to attend and secure scene)</p>	<p>Interim DI ADMIN 45-2 Incident reporting and management</p> <p>Sentinel Report: AE 527</p> <p>Defence casualty and bereavement support manual</p> <p>Where relevant:</p> <p>eDEOP 101 - Department of Defence Explosives Regulations Regulation 1.3</p> <p>Defence aviation safety manual</p> <p>Defence security manual</p>

6	<p>An incident deemed by commanders or managers to be serious, sensitive or urgent, not covered by the definitions above. That is, one that may bring Defence into disrepute; attract adverse media or parliamentary attention; or may adversely affect the efficiency of Defence, or impact on operational effectiveness or capability</p>	<p>Action: Line management/chain of command</p>	<p>Interim DI ADMIN 45-2 Incident reporting and management Defence security manual Sentinel Report: AE 527</p>
---	---	--	--

