Australian Government

Defence

INCIDENT REPORTING AND MANAGEMENT POLICY

This interim policy is a temporary replacement for the 2020 Incident Reporting and Management Manual. It will be reviewed and replaced in 2023.

AG4 in Defence Instruction – Administrative Policy prescribes and proscribes particular conduct relating to reporting, recording and managing incidents in Defence.

Mr David Haddad
Acting First Assistant Secretary
Defence Integrity

Department of Defence
CANBERRA ACT 2600

5 August 2022

ONE DEFENCE
WITH INTEGRITY

AMENDMENT CERTIFICATE

Amendment number	Chapter(s)	Amendment	Effected date
1	1	Inclusion of Prescribed Serious Operational Incident (PSOI) reporting and definition	22 June 2023

INTERIM INCIDENT REPORTING AND MANAGEMENT POLICY

Issued by:	This interim policy has been issued by the Acting First Assistant Secretary Defence Integrity with the authority of the Associate Secretary.
Purpose:	This interim policy document is a temporary replacement for AL2 of the Incident and Reporting Management Manual. It details policy and process relating to reporting, recording and managing incidents within Defence. It promotes compliance with AG4 of Defence Instruction – Administrative policy. The policy includes guidance to all Defence Personnel on what constitutes an incident and how those incidents are to be reported. The policy 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 incidents within Defence and externally, where appropriate.
Scope and applicability:	This policy is an administrative policy framework document. It applies to all Defence personnel. The terms of a relevant contract may extend the application of this policy to a person/s engaged under a contract. Defence Instruction – Administrative policy should be read in conjunction with this policy. In accordance with Defence Instruction – Administrative Policy, the Secretary and the CDF expect Defence personnel to comply with this policy. Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include the requirement to comply. If so, include such terms in the contract.
Management:	This interim policy will be reviewed and replaced by a policy that is properly aligned to the Administrative Policy Framework in 2023. The 2023 policy will be supported by suitably designed enabling products.
Availability:	This policy is available at Defence documents. 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 Defence Integrity
Policy contact:	Director Integrity, Policy and Industry Engagement – defence.integrity@defence.gov.au
Cancellation:	This interim policy is a temporary replacement for the Incident Reporting and Management Manual AL2
Definitions:	Definitions that apply to this Policy are at Annex 1A.
Related Documents:	A list of related documents can be found on the Defence Integrity Division intranet site.

ANNEX 1A

DEFINITIONS

The following list of terms are defined in Defence Instruction – Administrative policy. The definitions are intended to apply to their use in administrative policy framework documents:

Accountable officer
Administrative policy
Administrative policy framework
A person/s engaged under a contract
Australian Public Service employee
Commander
Defence
Defence civilian
Defence locally engaged employee
Defence member
Defence personnel
Defence-wide document
Framework documents
Manager
Personal information
Policy domain
Policy owner
Provision
Sensitive information
Supervisor
Technical authority

For the purpose of the policies described in this document, additional definitions[1] are applicable.

[1] Incident Reporting and Management Definitions

CONTENTS

CHAPTER 1

INCIDENT REPORTING BY DEFENCE PERSONNEL

INTRODUCTION

1.1 As defined within the Incident Reporting and Management Definitions, 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. It includes all complaints made by Defence Personnel, person/s engaged under a contract, people involved in Australian Defence Force cadets and other Defence supported youth programs, and members of the public, where the complaint is about Defence (including complaints about Defence Personnel).

REQUIREMENT FOR DEFENCE PERSONNEL TO REPORT AN INCIDENT

1.2 All Defence Personnel who have a reasonable suspicion that an incident has occurred, or who have received sufficient 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. If the incident involves one or more youth, immediate reporting requirements are specified in Youth Policy Manual (YOUTHPOLMAN) Part 1, Section 3, Chapters 3 and 4.

EXCEPTIONS TO REPORTING REQUIREMENT

1.3 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:

a. the incident is a Notifiable Incident[2] and is reported directly to a Defence Investigative Authority[3]

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*[4]

d. an incident that might affect a person's suitability to hold a security clearance is reported directly to the Australian Government Security Vetting Agency

or

e. a complaint of unacceptable behaviour has already been made to the complainant's or respondent's manager.

[2] Incident Reporting and Management Definitions

[3] Incident Reporting and Management Definitions

[4] https://www.legislation.gov.au/Details/C2021C00428

Further guidance on these exceptions is provided in the paragraphs below.

REPORTING A NOTIFIABLE INCIDENT DIRECTLY TO A DEFENCE INVESTIGATIVE AUTHORITY

1.4 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 the Joint Military Police Unit; 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).

1.5 Defence expects 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.

1.6 Comprehensive guidance on the reporting of Notifiable Incidents can be found at Chapter 3 of this manual.

REPORTING TO CIVILIAN POLICE FORCES

1.7 In some circumstances, it may be appropriate for Defence Personnel to report a Notifiable Incident directly to civilian police forces.

Example

An ADFA volleyball team, consisting predominantly of first year cadets, is on a training camp at Singleton. Late one evening, a 17 year old cadet reports that their volleyball coach, who is an ADFA staff member, assaulted them following a training session earlier that day. The cadet also notes that they witnessed the coach assault another ADFA staff member that afternoon. The Commanding Officer believes, due to immediate concerns for the safety of youth and ADF members, that an urgent response by civilian police is necessary. The CO calls civilian police using the usual police emergency contact number.

1.8 Nothing in this manual is intended to prevent Defence Personnel from reporting suspected criminal offences directly to civilian police. 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.

1.9 For any incidents involving persons (as respondents or claimants) under the age of 18, refer to paragraph 1.19.

REPORTING A PUBLIC INTEREST DISCLOSURE

1.10 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.

1.11 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.

1.12 Defence has implemented the *Public Interest Disclosure Act 2013* through the operation of the Defence Public Interest Disclosure Scheme[5]. Further information is available on the Defence Public Interest Disclosure Scheme intranet site or the Commonwealth Ombudsman's[6] website.

REPORTING A PRESCRIBED SERIOUS OPERATIONAL INCIDENT

1.13 Defence Personnel can report a Prescribed Serious Operational Incident (PSOI) through their supervisor or operational chain of command.

1.14 There are two reporting processes that may be used by Defence Personnel that are independent from the normal chain of command:

a. There will be circumstances where it is appropriate for Defence Personnel to report a PSOI directly to a Defence Investigative Authority such as Military Police.

b. The Public Interest Disclosure (PID) Scheme also provides an appropriate process for Defence personnel to report PSOI.

1.15 The PID Scheme provides specific protections for disclosers. PID reports are received and managed independently from the chain of command. Further information is available on the Defence Public Interest Disclosure Scheme intranet site or the Commonwealth Ombudsman's website.

REPORTING SECURITY RELATED INCIDENTS

1.16 Security related incidents can constitute an exception to the mandatory reporting requirement as detailed in the Defence Instruction Administrative Policy Annex C –AG4- Incident reporting and management. Guidance on reporting security related incidents can be found in the Defence Security Principles Framework[7].

1.17 Defence Personnel reporting incidents in compliance with Control 77.1 Security Incident Management and Investigation are considered to have met their obligation to report an incident.

REPORTING SUSPECTED UNACCEPTABLE BEHAVIOUR

1.18 The Defence policy on reporting unacceptable behaviour is detailed in the Defence Instruction Administrative Policy Annex J –PPL7 – Required behaviours in Defence and the Complaints and Alternative Resolutions Manual[8].

1.19 Defence Personnel reporting unacceptable behaviour may report the unacceptable behaviour 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. Commanders and managers may subsequently identify additional reporting requirements (see Chapter 3 of this manual).

[5] http://drnet/AssociateSecretary/integrity-assurance/Fraud-Corruption/Pages/Public-Interest-Disclosure.aspx

[6] https://www.ombudsman.gov.au/Our-responsibilities/making-a-disclosure

[7] http://intranet.defence.gov.au/home/documents/home/publications/policy-documents/defence-security-principles-framework.htm

[8] http://drnet.defence.gov.au/People/ComplaintResolution/Complaints-and-Alternative-Resolutions-Manual-(CARM)/Pages/Complaints-and-Alternative-Resolutions-Manual-(CARM).aspx

VICTIMS OF PHYSICAL VIOLENCE OR EMOTIONAL TRAUMA

1.20 Defence Personnel who are victims of physical violence or emotional trauma arising from the commission of a criminal act are not compelled to report the incident in accordance with Defence policy; however such victims are encouraged to report incidents to their managers and commanders.

INCIDENTS INVOLVING PERSONS UNDER 18 YEARS OF AGE

1.21 For any incidents involving persons (as respondents or claimants) under the age of 18, actions must be taken in accordance with the guidance provided in YOUTHPOLMAN Part 1, Section 3, Chapters 3 and 4 and this manual.

1.22 Specific caution is required in relation to the disclosure of certain personal information when reporting on youth.

CHAPTER 2

INCIDENT RECORDING AND MANAGEMENT BY MANAGERS AND COMMANDERS

INTRODUCTION

2.1 The responsibility for recording a Defence Incident Record 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 If the incident involves one or more youth, additional reporting requirements are specified in YOUTHPOLMAN Part 1, Section 3, Chapters 3 and 4.

2.3 The authorised case management system for centralised incident recording in Defence is the Defence Policing and Security Management System. For youth protection events/incidents, refer to YOUTHPOLMAN Part 1, Section 3, Chapters 3 and 4.

2.4 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.

2.5 Where an incident is recorded in the Army Incident Management System there is no requirement to raise a Defence Incident Record.

GROUP AND SERVICE RESPONSIBILITIES

2.6 Each Group and Service must appoint at least one Defence Incident Record Manager. Where a Defence Incident Record Manager has not been appointed, the role will be performed by the Chief of Staff in each Group and Service.

2.7 While managers and commanders are responsible for ensuring all Defence Incident Records are recorded in the Defence Policing and Security Management System, Group Heads and Service Chiefs may implement Group or Service specific standard operating procedures or protocols for incident record management. Head Joint Support Services Division must be informed of certain youth protection events/incidents; refer to YOUTHPOLMAN Part 1, Section 3, Chapter 3.

DEFENCE INVESTIGATIVE AUTHORITY RESPONSIBILITIES

2.8 On receipt of a report of a Notifiable Incident, 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.

THE DEFENCE INCIDENT RECORD

2.9 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.

2.10 A Defence Incident Record is not substituted by other operational reporting methods where an Operational Authority may be alerted to an incident by phone, email or formal messaging (Signals). A Defence Incident Record process will always need to be submitted, with the relevant Service headquarters kept informed.

2.11 A Defence Incident Record **must** be 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.

2.12 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 minimal 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.

2.13 Managers and commanders must ensure all incidents reported to them are recorded in the Defence Policing and Security Management System using the link to the Defence Incident Record. A Defence Incident Record **must** be completed at the earliest opportunity. Where access to the Defence Policing and Security Management System is not possible, Defence Personnel should complete a Form AE530 – Defence Incident Record[9] and upload the details of that form into the Defence Policing and Security Management System using the Defence Incident Record link when available.

2.14 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.

[9] https://formsportal.dpe.protected.mil.au/bin/forms-portal/form?AE530

2.15 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 Control 77.1 Security Incident Management and Investigation which are recorded in the Defence Policing and Security Management System using form XP188 (Security Report).

b. Information disclosed by Defence Personnel to their supervisors[1] under the *Public Interest Disclosure Act 2013*, is then 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 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.

INFORMATION REQUIRED FOR COMPLETION OF A DEFENCE INCIDENT RECORD

2.16 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). Refer to paragraph 1.29 for incidents involving persons under the age of 18;

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 numbers to any records containing more detailed information about the incident (e.g. the ComTrack receipt number, Sentinel event number etc.).

---

[10] Supervisors in Defence should be aware of their obligations under the Public Interest Disclosure Act. Supervisors can review the Public Interest Disclosure Act or access guidance on the Defence Public Interest Disclosure Scheme intranet website or the Commonwealth Ombudsman's website.

2.17 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 Policy Framework and the Defence Records Management Policy for further information]. Where the Notifiable Incident involves a respondent or claimant under 18, it is essential that managers and commanders read part 1 of the Youth Policy Manual (including policy on disclosure of certain personal information).

THE DEFENCE INCIDENT RECORD PROCESS

2.18 Defence Incident Records are to be completed in three stages: initial; update and closure. The Defence Policing and Security Management System provides for each stage to be recorded.

Initial: Provides the known facts of any incident on a who, what, where, and when basis. It is acknowledged that the initial Defence Incident Record may be incorrect or contain inaccuracies.

Update(s): Records any developments regarding an incident including what, if any, further action is underway or is required. An update can also be used to correct information provided in the initial report. 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.

2.19 In some minor circumstances, only an initial Defence Incident Record need be completed. When this situation occurs the Defence Incident Record should be annotated as initial and closure.

2.20 For incidents where responsibility for the management of involved personnel is transferred to a different line management or chain of command, the losing area is responsible for conducting a formal handover process to the gaining area. The handover must ensure alignment of the Defence Incident Record numbering and data entry into the Defence Policing and Security Management System, as well as ensuring that final notification of incident outcomes and resolution is provided to the Defence Incident Record originator.

2.21 Further guidance on the use and management of Defence Incident Records is available by downloading the ‘How to Submit a DIR’ within the Defence Incident Record intranet page.

2.22 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 AE527 – Sentinel event report

b. a report of unacceptable behaviour selecting and using the ComTrack Self Service through an individual’s PMKeyS Portal

c. a Notifiable Incident with mandatory notification requirements to a Defence Investigative Authority

d. a casualty incident as required in the Defence Casualty Manual

or

e. any other mandated reporting and recording requirements necessary under legislation or extant policy.

SHARING OF DEFENCE INCIDENT RECORDS ACROSS SERVICES AND GROUPS

2.23 For incidents occurring within a particular Group or Service but which involve personnel from another Group or Service, the reporting Group or Service must ensure that all other relevant Group or Service headquarters are included during the initial notification process. The reporting Group or Service must also keep other relevant Group or Service headquarters updated through to the closure and/or handover of the incident.

FACT FINDING

2.24 As a tool in determining the content of a Defence Incident Record or to decide whether an incident is a Notifiable Incident as described in Chapter 1 of this manual, managers and commanders may wish to conduct ‘fact finding’. Fact finding is a process of collecting information to support decision-making. However, an initial Defence Incident Record should not be delayed merely to collect additional information.

2.25 Guidance on the use of fact finding to assist decision-making is available in the Good Decision-Making in Defence guide.

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.

3.2 Where a Notifiable Incident involves a respondent or claimant under 18, refer to YOUTHPOLMAN Part 1.

NOTIFIABLE INCIDENTS

3.3 The definition of Notifiable Incidents can be found in the Definitions section of this Manual.

3.4 Defence personnel are required to report all Notifiable Incidents in accordance with this manual.

RESPONSIBILITIES OF MANAGERS AND COMMANDERS

3.5 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 must 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 in appropriate cases. Legal and medical professional privilege may preclude the reporting of certain information.

3.6 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. Further detail can be found in the Notifiable Incident Referral Guide.

3.7 In dealing with reported incidents including Notifiable Incidents, managers and commanders should refer to the Notifiable Incident Referral Guide to determine the most appropriate Defence Investigative Authority or support agency to which the incident should be referred.

3.8 The lead authority for the investigation of fraud and fraud-related matters is the First Assistant Secretary Defence Integrity. Under the authority of the First Assistant Secretary Defence Integrity, responsibility for undertaking fraud investigations is shared between the four Defence Investigative Authorities: the Fraud Control and Investigations Branch (Defence Integrity Division); Joint Military Police Unit; Directorate Conduct and Performance (Defence People Group); and in limited circumstances Security Threat and Assurance Branch (Defence Security Division).

3.9 Consideration should be given to the circumstances of the alleged fraud or corruption, with the possibility of joint investigations, to achieve the best outcome for Defence. Due to the complex nature of fraud and corruption, it is essential for each Defence Investigative Authority to consider jurisdictional issues as outlined in this chapter.

3.10 In circumstances where the jurisdiction for investigating a Notifiable Incident is not clear, managers and commanders must report the Notifiable Incident to a Defence Investigative Authority. Defence expects the Defence Investigative Authority receiving the report to engage with other Defence Investigative Authorities, as appropriate.

3.11 Fraud Control and Investigations Branch, Defence Integrity Division, is responsible for the investigation of serious and complex fraud, corruption and misconduct allegations. Consultation between Defence Investigative Authorities may be required to determine where the jurisdiction for investigation and prosecution should be, based on the seriousness and complexity of the matter.

3.12 Under the *Defence Force Discipline Act 1982*, the Joint Military Police Unit is responsible for investigating allegations of routine and minor offences of fraud by ADF members, with copies of Investigation Reports provided to Fraud Control and Investigations Branch (Defence Integrity Division).

3.13 Matters pertaining to ADF members suspected of committing fraud offences of a serious or complex nature, containing elements of corruption or potentially politically sensitive matters are to be discussed between the Joint Military Police Unit and Fraud Control and Investigations Branch (Defence Integrity Division).

3.14 Defence Security Division is responsible for the management of reported security incidents. Security incidents assessed as meeting serious and complex thresholds for investigation will generally be escalated to a security investigation managed by Defence Security Division.

3.15 Managers and commanders must afford all reasonable assistance to the relevant Defence Investigative Authority in the execution of their duties to prevent any unreasonable impediment or interference, including directing or obstructing the investigation or inquiry process.

3.16 Managers and commanders retain responsibility for monitoring and reporting on all incidents to line management and chain of command.

HOW TO REPORT A NOTIFIABLE INCIDENT

3.17 A report of a Notifiable Incident should be made by the most expeditious means possible in accordance with the Notifiable Incident Referral Guide. To ensure there is an auditable reporting trail, reports should be made in writing (for example by email, message, minute 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 must not be unduly delayed.

ACTIONS ON REPORTING A NOTIFIABLE INCIDENT

3.18 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.

3.19 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 the Defence Incident Scene Initial Action and Preservation Manual 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 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.