The Auditor-General
Audit Report No.14 2013–14
Performance Audit

Explosive Ordnance and Weapons Security Incident Reporting

Department of Defence

Australian National Audit Office

ISSN 1036–7632
ISBN 0 642 81416 3 (Print)
ISBN 0 642 81417 1 (Online)

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:
publications@anao.gov.au

Canberra ACT
18 December 2013

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Defence in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament. The report is titled *Explosive Ordnance and Weapons Security Incident Reporting*.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **publications@anao.gov.au**

ANAO audit reports and information about the ANAO are available on our website:

http://www.anao.gov.au

Audit Team
Natalie Whiteley
Kim Murray
Stuart Turnbull

Contents

Tables

Figures

Abbreviations

ADF	Australian Defence Force
ADFIS	Australian Defence Force Investigative Service
ANAO	Australian National Audit Office
CDF	Chief of the Defence Force
DI(G)	Defence Instruction (General)
DEOC	Defence Explosive Ordnance Committee
DEOP 101	Defence Explosive Ordnance Publication 101
DFD Act	*Defence Force Discipline Act 1982*
DIA	Defence Investigation Authority
DSA	Defence Security Authority
dsaARMS	Defence Security Authority Audit Recommendation Management System
DSM	Defence Security Manual
DPSMS	Defence Policing and Security Management System
EO	Explosive ordnance
EOIAC	Explosive Ordnance Incident Administration Cell
FFE	Free from explosives
JLC	Joint Logistics Command
PSPF	Protective Security Policy Framework
VCDF	Vice Chief of the Defence Force
WME	Weapons, munitions and explosives

Summary and Recommendations

Summary

Introduction

1. The effective management of explosive ordnance (EO) and weapons is integral to military capability and operations, and contributes to the safety of Australian Defence Force (ADF) members and the public.[1] The Department of Defence (Defence) should appropriately manage and account for its diverse inventory of EO and weapons to ensure these items are readily available to the ADF when required. EO and weapons held by Defence also pose potential risks to ADF members and public safety if they are mishandled or fall into the hands of those seeking to misuse them. Experience has shown that the barrier between Defence and the community is a permeable one that can be breached accidentally or deliberately.[2]

2. The management of EO and weapons primarily relies on the design and application of appropriate controls throughout their life cycle, from procurement, storage and handling, through to final use or disposal. A necessary complement to these arrangements is a reliable system for recording and reporting security incidents involving EO and weapons in the event of control failures. Such a system should provide senior management in Defence with visibility of these incidents and their outcomes, and inform the development and application of the procedures used by Defence to store, handle and account for EO and weapons.

[1] Explosive ordnance (EO) is defined as all munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. Examples include missiles, torpedoes, mines and flares. Defence's definition of EO also includes similar and related non-explosive EO items and components (for example, containers and packaging). The term 'weapon' includes both a 'Defence weapon' and a 'cadet firearm'. See Appendix 2 for Defence's detailed definitions of EO and weapons.

[2] In addition to historical EO and weapons discovered periodically in the community (such as munitions found on old training sites or equipment retained by previous generations of ADF personnel), modern EO and weapons can surface in the wider community as a result of misappropriation, malfunction or loss.

3. The Defence Security Manual (DSM) is the authoritative policy for the reporting of security incidents within Defence.[3] The DSM defines the following EO and weapons security incidents as major security incidents with consequential reporting requirements:

- Any actual or suspected loss, theft, attempted theft, recovery of, or suspicious incidents involving EO, Defence weapons, associated equipment or cadet firearms.
- The discovery of EO or weapons; actual or attempted break-ins to licensed EO facilities, armouries or weapons storage facilities; and loss, compromise or theft of any keys, cards or other access devices associated with EO and weapons security and storage.
- The inappropriate handling and storage of EO, weapons and associated equipment related to EO and weapons.

4. Defence recorded 960 EO and weapons security incident reports between 1 January 2011 and 28 August 2013. Common examples of the security incidents included items found on, or missing from, Defence premises, such as small arms ammunition, grenades and plastic explosives; and the recovery of World War II munitions in public areas. Two of the most significant security incidents during the period were the discovery of a live in-service grenade in a public area and the loss of an in-service Claymore antipersonnel weapon. Many of the EO and weapons security incidents were multifaceted and had a range of implications for Defence including, for example, issues of safety and proper conduct.

Organisational arrangements for EO and weapons security incidents

5. As a large and dispersed organisation, Defence must have appropriate arrangements in place to provide both local control and effective whole-of-Defence oversight and assurance of the management of EO and weapons. Defence's arrangements for managing EO and weapons security incidents involve a broad range of internal management structures, internal stakeholders and activities.

[3] Department of Defence, Defence Security Manual, September 2012.

6. The Defence Security Authority (DSA) is the central point of contact for protective security matters in Defence. The DSA is led by Defence's Chief Security Officer and is responsible for, among other things:

- setting Defence protective security policy including Defence's primary source of protective security policy, the DSM; and
- monitoring and reporting on Defence's security compliance, performance and risks, including managing the Defence Security Authority Audit Recommendation Management System (dsaARMS) and compiling regular reports on EO and weapons security incidents for the Defence Explosive Ordnance Committee (DEOC).

7. Defence policy requires the reporting of all major security incidents to the DSA. The DSA is responsible for: ensuring that reported security incidents have been entered into the Defence Policing and Security Management System (DPSMS)[4]; analysing all reported security incidents; and determining the incidents that need to be investigated and the most appropriate Defence Investigation Authority (DIA)[5], Civil Authority or ADF unit to conduct an investigation or administrative inquiry.

8. In August 2007, Defence completed a comprehensive internal performance audit of its management of weapons, munitions and explosives (WME).[6] The audit made 58 recommendations focused on improving Defence's policies and systems for the management and accounting of WME to enhance visibility and control throughout their life cycle. The audit made a number of recommendations to strengthen the role and capability of the DSA in the areas of audit, review, compliance and remediation of WME security.

[4] The Defence Policing and Security Management System (DPSMS) is Defence's primary computerised system for recording all reports of, and investigations into, major security incidents.

[5] The Security Investigations Unit in the DSA is one of the six DIAs. The other DIAs are the Australian Defence Force Investigative Service (ADFIS); the Service police organisations of the Army, Air Force and Navy; and the Directorate of Investigation and Recovery within the Inspector General Division. The DIAs are authorised by the Secretary of Defence and the Chief of the Defence Force (CDF) to conduct formal investigations, including into EO and weapons security incidents.

[6] Department of Defence, 'Security Performance Audit of Weapons Munitions and Explosives', 17 August 2007. This audit was initiated following advice from the Australian Federal Police (AFP) to Defence of a police investigation into the source of a military rocket launcher in the possession of criminal elements, which the AFP believed could have been of ADF origin. A subsequent ADF and AFP investigation confirmed that the weapon was of ADF origin and thought by Defence to have been disposed of some years earlier. In 2008, a serving Army officer received a jail sentence for the theft and sale of the item. The impact of the theft is ongoing as not all of the stolen weapons have been recovered.

Audit objective, criteria and scope

9. The audit objective was to assess the effectiveness of Defence's arrangements for monitoring and reporting EO and weapons security incidents. To reach a conclusion against the audit objective, the following high level audit criteria were used:

- documentation and advice provided to Defence personnel to assist them in reporting EO and weapons security incidents is adequate;
- Defence's reporting arrangements for EO and weapons security incidents are operating effectively (including the processes for Defence personnel to report EO and weapons security incidents, and the process for reporting data on EO and weapons security incidents to the Defence Executive and relevant Defence committees);
- Defence's system for recording details of EO and weapons security incidents is adequate; and
- the DSA's process for recording, reporting, and responding to the outcomes of investigations into EO and weapons security incidents supports continuous improvement in EO and weapons security incident management.

10. The audit also reviewed Defence's progress in addressing the two relevant recommendations from ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*. The two recommendations were that Defence:

- take steps to remove all the inconsistencies in the definitions and requirements for the management of EO security incidents in Defence policy and procedural documents (Recommendation No.4); and
- improve its incident reporting and data management of EO security incidents (Recommendation No.5).[7]

11. The audit focused on the central administration of EO and weapons security incident reporting in Defence by the DSA, and the arrangements in

[7] ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*, April 2011.

place to assist Defence personnel in reporting incidents.[8] The audit did not assess the extent to which all EO and weapons security incidents are reported.

Overall conclusion

12. Defence has diverse EO and weapons holdings throughout Australia and internationally. The secure and effective management of these holdings contributes to national security, military capability and operations, and the safety of ADF members and the public. The implementation of an appropriate control framework covering the storage and transport, usage and disposal of EO and weapons is an essential aspect of their management. Defence security incident reporting and investigations complement these arrangements and provide a means for Defence to understand control failures and inform remedial action, including the identification of opportunities for improvement in the design and application of controls.

13. Experience has shown that EO and weapons security incidents occur relatively frequently and they may have potentially serious consequences. Between 1 January 2011 and 28 August 2013, Defence recorded 960 EO and weapons security incident reports, ranging from the discovery of historical EO and weapons in the community, to the mishandling and misplacement of EO and weapons currently in-service with the ADF.

14. Defence's arrangements for monitoring and reporting EO and weapons security incidents have only been partially effective in enabling Defence to: centrally identify EO and weapons security incidents, maintain a complete and accurate record of these incidents, and identify and address the underlying causes of incidents.

15. Within Defence's overall framework for EO and weapons security, the DSA has responsibility for the central monitoring of security incidents and developing Defence-wide protective security policy. The effectiveness of the DSA in fulfilling these functions is dependent on clear security incident reporting requirements, the completion of security incident reports by Defence personnel in accordance with these requirements, and a sound approach to recording details of incidents and investigations, analysing this data and responding appropriately.

[8] The audit did not examine controls of EO and weapons, such as Defence's security arrangements for storing or transporting EO or weapons and ADF base security arrangements.

16. As part of the framework, Defence has a suite of whole-of-Defence and local policies and guidance available to staff on identifying and reporting EO and weapons security incidents. This suite of policies and guidance reflects different lines of reporting and accountability for the management of EO and weapons under the chain of command for each service, to the Vice Chief of the Defence Force[9] and to the DSA for security incidents. However, there is fragmentation and a general lack of coordination in these reporting arrangements, characterised by differing reporting requirements and methods. There is scope for Defence to streamline reporting requirements in order to facilitate timely and complete EO and weapons security incident reporting.

17. Defence policy mandates the reporting of all EO and weapons security incidents to the DSA to enable the DSA to monitor and triage[10] these incidents. While incident reporting and management generally occurs at an ADF Service and Defence Group level, reporting is often incomplete because there is regular non-compliance with the requirement to inform the DSA about EO and weapons security incidents. For 27 per cent (186 of the 693) of the EO and weapons security incident reports completed across Defence between 1 January 2011 and 25 March 2013[11], the DSA was not notified in accordance with Defence's reporting requirements. During the course of the audit, Defence identified a further 162 EO security incidents for the period January to March 2013 which had not been recorded as security incidents or reported to the DSA in accordance with Defence requirements.[12] The DSA investigation into the non-reporting of these additional EO security incidents to the DSA, showed that the non-reporting was widespread, and extended over a more prolonged period[13], representing a systemic level of non-compliance with the current and mandatory Defence-wide policy issued by the Secretary and CDF.[14] These

[9] Defence refers to the Vice Chief of the Defence Force as the single point of accountability for EO in Defence.

[10] Triaging relates to the process of assessing incidents to determine the order and priority of their treatment and investigation.

[11] As part of this audit, the ANAO reviewed Defence data on 693 security incident reports covering the period 1 January 2011 to 25 March 2013.

[12] However, the 162 incidents were reported as EO incidents through other EO reporting channels to other areas of Defence.

[13] The Defence units involved respond to approximately 700 EO incidents per year—the majority of which should have been identified as major security incidents and reported to the DSA. However, the DSA investigation found that almost none of these incidents had been reported to the DSA by the proper channels in accordance with existing policy.

[14] While a DSA investigation into the non-reporting of the security incidents is ongoing, it also indicates that the areas of Defence involved were selective in their application of reporting requirements.

shortcomings in the reporting of EO and weapons security incidents compromise the integrity of the central monitoring and reporting system and have detracted from the DSA's capacity to fulfil its central monitoring role.

18. Defence has established a primary electronic system for recording details of all EO and weapons security incidents and investigations, known as the Defence Policing and Security Management System (DPSMS). This system has the potential to provide for central visibility over incidents amidst diverse lines of reporting and accountability. However, the 162 EO security incidents identified during the audit were not recorded in DPSMS and data quality for recorded incidents has been an ongoing issue, with 73 per cent of EO and weapons security incident reports during the period under review requiring some form of data correction. In addition to DPSMS, Defence uses other electronic systems to record details of EO and weapons security incidents but does not formally share and align the information contained in those systems and DPSMS, creating an additional risk of inconsistent and incomplete data in DPSMS. Further, only a small number of DSA staff have broad access to comprehensive records of all EO and weapons security incidents and investigations entered into DPSMS by the various Defence Investigative Authorities (DIAs), and the DSA does not routinely analyse this data. These recording and access arrangements, which are characterised by fragmentation, incomplete data entry and the need for rework, are generally inefficient and not conducive to a whole-of-Defence understanding of the underlying causes and outcomes of EO and weapons security incidents and investigations, and any associated trends. They are also an impediment to establishing a viable feedback loop informing Defence policy and the implementation of the framework for EO and weapons security and control.

19. In 2013, Defence reviewed its implementation of the 58 recommendations from the 2007 Defence internal performance audit on the management of WME security. This review indicated that work remains for Defence to implement, or demonstrate implementation of, almost half of the 58 recommendations. The Defence reviews highlighted the existence of 'upstream' risks to Defence's EO and weapons management in terms of how EO and weapons are stored, handled, transported and accounted for. These risks, coupled with the shortcomings in the current 'downstream' monitoring and reporting of EO and weapons security incidents identified in this audit, highlight that Defence still has some way to go to achieve confidence in the effectiveness of its EO and weapons security arrangements. The DSA is not yet fulfilling the strong role envisaged at the time of the 2007 review in the areas of audit, review, compliance and remediation of WME security.[15] Symptomatic of this situation, the ADF has conducted periodic amnesties–for EO inappropriately held by personnel–without the knowledge of the DSA[16], and without centrally tracking the amnesties or centrally reporting the items recovered.

20. Defence has established central reporting processes and systems at considerable cost in an attempt to achieve an understanding of the occurrence, underlying causes and outcomes of EO and weapons security incidents and investigations across Defence, and any associated trends in these incidents. The efficient and effective operation of its central arrangements will help Defence realise their full potential in support of the ADF, particularly through establishing a robust feedback loop to inform Defence policy and the implementation of the EO and weapons control and security framework. In a resource constrained environment, streamlining reporting and co-ordination arrangements offers an opportunity for Defence to leverage its investment in centralised processes and systems to more effectively mitigate control risks and achieve efficiencies in local and Defence-wide security incident reporting arrangements.

21. The ANAO has made two recommendations directed towards Defence streamlining EO and weapons security incident reporting requirements and strengthening central visibility of EO amnesties. In addition, Recommendation No.5 from ANAO Report No. 37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy* remains relevant—that Defence improve its incident reporting and data management for EO security incidents.

Key findings by chapter

Reporting EO and weapons security incidents (Chapter 2)

22. The primary sources of Defence's EO and weapons security incident reporting requirements are the DSM and the Defence Instruction (General) DI(G) ADMIN 45-2 'The reporting and management of notifiable incidents'. Some of the reporting requirements in these two policy documents are the same and others differ. ANAO Audit Report No.37, 2010–11, *Management of Explosive*

[15] Defence has noted that the Chief Security Officer made a decision to take DSA staff offline in September 2011 to undertake a higher priority task and they only returned to their routine duties at the end of March 2013.

[16] The DSA advised the ANAO that it was not aware of when amnesties occurred, the frequency of amnesties or how they have been managed.

Ordnance Held by the Air Force, Army and Navy included a recommendation (Recommendation No.4) that Defence take steps to remove all the inconsistencies in the definitions and requirements for the management of EO security incidents in Defence policy and procedural documents. While the DSM has been amended to this end, the content of DI(G) ADMIN 45-2 has not changed since its last revision in March 2010[17], and there remains scope for Defence to further streamline the requirements in this document and harmonise them with those set out in the revised DSM. Defence's documentation on its process to address ANAO Recommendation No.4 suggests that despite best efforts in some areas of Defence, the fragmented nature of the 'ownership' of Defence policy and procedures continues to challenge Defence's capacity to rationalise and align its requirements for managing and reporting EO and weapons security incidents, and its ability to do so in a timely way.[18]

23. Based on the requirements of the DSM and DI(G) ADMIN 45-2, EO and weapons security incidents should be reported to up to eight separate stakeholders using a range of methods, reflecting a general lack of coordination and fragmentation in the reporting arrangements. This situation has contributed to non-compliance with individual reporting requirements, and the emergence of coordination issues relating to the notification of Defence stakeholders and investigators. In order to facilitate timely and complete EO and weapons security incident reporting and an improvement in the DSA's visibility over these incidents, Defence should streamline reporting requirements. There is also scope to improve arrangements to coordinate the dissemination of reported information to relevant Defence stakeholders.

24. Defence policy provides ADF unit managers with the option to declare periodic amnesties on EO held by personnel but not authorised for retention, which is a potentially beneficial arrangement. However, there are currently no mechanisms in place to centrally track the number of amnesties declared or the types of EO involved. There are also no formal requirements to centrally report EO items recovered through amnesty arrangements. In consequence, there is no process to acquit for items surrendered during an amnesty, and to reconcile Defence-wide records of EO items. To further contribute to Defence's visibility

[17] DI(G) ADMIN 45-2 has also now passed its review date of 30 March 2013. In September 2013, Defence informed the ANAO that it is reviewing a range of issues relating to reporting and management of matters for investigation, and that it has deferred the review of the instruction until there is greater clarity on these issues.

[18] This challenge primarily relates to Defence's efforts to align the requirements of the DSM (which is 'owned' by the DSA) and the DI(G) (which is 'owned' by the Inspector General Defence).

over EO security incidents and account for items recovered, Defence should establish a formal reporting and acquittal process for EO amnesties.

25. On 20 June 2013, in the course of the audit, Defence informed the ANAO that it is working on establishing a formal reporting process for EO amnesties. Defence noted that this may require changes to key policy documents such as the DSM, and acknowledged that it is important to have the process in place before the return of troops from Afghanistan.

26. The DSA's Security Incident Centre is responsible for the assessment, referral and analysis of all major security incidents in Defence. Defence identified 194 EO and weapons security incidents reported in DPSMS between 1 January 2011 and 25 March 2013, for which primary responsibility rested with a DIA other than the Security Incident Centre. Of these 194 incidents, only 25 (13 per cent) contained information indicating that the DSA carried out some form of initial assessment.[19] Similarly, the DSA has identified 186 EO and weapons security incidents not reported to the DSA in accordance with the DSM between January 2011 and March 2013.[20] Consequently, many EO and weapons security incidents are assessed, managed, investigated and/or closed by other DIAs without an initial assessment by the Security Incident Centre, contrary to Defence requirements.

27. During the audit, Defence informed the ANAO of 162 EO security incidents for the period January to March 2013, in addition to those discussed in paragraph 26, which were not reported to the DSA in accordance with Defence reporting requirements.[21] The types of EO involved in these incidents were largely small arms rounds, but also included other in-service, recently out-of-service and obsolete EO including some projectiles, grenades, mortars, flares and fuses. A DSA investigation into the non-reporting was finalised in early December 2013. Analysis by the DSA of the EO items involved has

[19] Defence informed the ANAO that it was possible that for some of the remaining 169 incidents there may have been DSA action that was not able to be identified through the DPSMS report, and that to identify these actions would require examination of each incident record in DPSMS.

[20] The DSA has access to security incident records that are created and managed by other DIAs and is therefore able to determine the number of security incidents that are not formally reported to the DSA in accordance with the DSM. Defence identified 186 such EO and weapons security incidents that were created by other DIAs on DPSMS.

[21] Defence informed the ANAO that following an examination of 177 EO security incidents, Defence had determined that 15 were reported via Significant Incident Reports to the Security Incident Centre, and the remaining 162 were reported as EO incidents through other EO reporting channels. Defence confirmed that the 162 EO security incidents were not reported to the DSA as required by Defence security incident reporting requirements.

determined that a large proportion of the incidents involved EO items that, due to their age, condition and/or origin, are not of significant consequence to Defence in relation to security vulnerabilities. Nonetheless, two of the incidents met the criteria for a DSA investigation, including the discovery of a live in-service grenade by a member of the public in a public area; and another nine incidents required further DSA assessment. The non-reporting of the security incidents to the DSA meant that it could not consider potential security vulnerabilities in a timely way.

28. The DSA informed the ANAO that one of the contributing factors to the non-reporting of incidents is that the area involved in the non-reporting was 'faced with an onerous task associated with recovery of EO, which includes the requirement to submit up to five separate reports, depending on the circumstances of an incident'. The DSA investigation into the non-reporting indicates that the areas of Defence involved were selective in their application of reporting requirements, and the ADF personnel involved made their own assessments on which EO incidents to report as security incidents to the DSA. The Defence units involved respond to approximately 700 EO incidents per year, the majority of which should have been identified as major security incidents and reported to the DSA. However, the DSA investigation found that almost none of these incidents had been reported to the DSA by the proper channels in accordance with existing policy.

29. Notwithstanding Defence's assessment of security vulnerabilities, the non-reporting of the EO security incidents to the DSA represents a systemic level of non-compliance with current and mandatory Defence-wide policy issued by the Secretary and CDF. As a result of the findings from Defence's investigation into the non-reporting of the EO security incidents, the DSA is proposing that Defence undertake a number of policy changes such as simplifying reporting arrangements and revising existing policy documents to remove ambiguity. There would be merit in Defence following-up on these initiatives, and any related reform initiatives, through its internal audit function.

Defence's information systems for recording EO and weapons security incidents and investigations (Chapter 3)

30. DPSMS is the primary and approved electronic system for recording all reports of, and investigations into, major security incidents within Defence. The quality of security incident data in DPSMS has been an ongoing issue, and was identified in ANAO Report No. 37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*. The ANAO recommended that Defence improve its incident reporting and data management for EO security incidents (Recommendation No.5).[22] In the context of a reporting framework which involves various DIAs entering data into DPSMS based on information provided by reporting areas, there is a shared responsibility to enter data accurately, and a central responsibility to periodically test the integrity of that data.

31. Over a number of years, the DSA has manually adjusted DPSMS data outside of the system in order to accurately report details of security incidents to senior management in Defence. The DSA sought to address data quality issues through a review of all security incident data in DPSMS for the period January 2011 to March 2013. Of the EO and weapons security incident reports examined as part of this review, 73 per cent required some form of data correction, reflecting ongoing issues around the efficiency and effectiveness of data entry. These findings and the significant breaches of EO security incident reporting requirements discussed in paragraph 27, show that Defence has not yet adequately implemented Recommendation No.5 from ANAO Report No. 37, 2010–11, to improve EO security incident reporting and data management. In its response to that recommendation, Defence could also consider reporting and data management for weapons security incidents.

32. Following its DPSMS data quality review, the DSA has undertaken further data quality checks and intends to institute a standard and regular quality assurance process to check data for all security incidents recorded in DPSMS. Introducing mandatory data fields for security incidents, and where practicable, automating data entry for these fields, would assist in improving the quality of the EO and weapons security incident data in DPSMS, and the efficiency of data entry.

33. Effective monitoring and analysis of its records of EO and weapons security incidents and resulting investigations can provide Defence with valuable information on the health of its security framework. However, only a small number of DSA staff have broad access to the EO and weapons security incidents and investigations data within DPSMS, and the DSA does not routinely analyse this data. Defence could therefore be missing opportunities

[22] At the time of ANAO Audit Report No.37, 2010–11, there was evidence that not all EO security incidents were being promptly reported to the DSA and the extant reporting examined by the ANAO showed some limitations. Defence was not able to provide the ANAO with complete and consistent data on EO security incidents, leading the ANAO to conclude that Defence had yet to achieve visibility of all EO security incidents.

to identify and manage risks, address systemic problems and make improvements to its EO and weapons security arrangements.

34. Reflecting the multifaceted nature of EO and weapons security incidents, and the range of accountabilities at an ADF Service and Defence Group level for managing EO and weapons, Defence uses multiple information systems to record details of these incidents. The use of multiple information systems needs to be well coordinated because it has the potential to undermine Defence's efforts to achieve central visibility of EO and weapons security incidents, and consequently the Department's efforts to monitor and manage the risks associated with these incidents. However, at present, no formal arrangements are in place to share and align the information recorded in the different systems.

EO and weapons security incident investigations (Chapter 4)

35. Defence has in place a range of policies, standards and procedures to guide the conduct of security investigations. These investigations are undertaken by six DIAs. There may be multiple inquiries and investigations of a single security incident undertaken by DIAs and ADF units, which address various considerations including appropriate administrative action. These arrangements highlight the challenge for the DSA in monitoring EO and weapons security incident investigations and following-up on their outcomes.

36. The DSA does monitor the overall numbers of EO and weapons security investigations in order to report these numbers to the Defence Executive. However, the DSA does not regularly monitor other DIAs' or ADF units' investigations and/or inquiries, nor are the outcomes routinely recorded against the DSA record for the investigation of that EO and weapons security incident. An examination of common themes emerging from EO and weapons security investigations across the DIAs would contribute to Defence's understanding of trends and potential issues leading to EO and weapons security incidents.

37. As part of this audit, the ANAO examined records of investigations into EO and weapons security incidents undertaken by the DSA from 1 January 2011 to 25 March 2013. During this period, there were 83 security investigations involving the loss, theft or recovery of EO and weapons. Of these 83 investigations, the DSA Security Investigations Unit was the primary case officer in 24 cases (29 per cent). The main reasons for conducting the DSA investigations included that: the EO or weapon(s) reported lost or stolen represented a significant risk to the community; there was a suspected level of criminality in the EO and weapons security incident; and there had been previous EO and weapons security incidents involving the unit or contractor.

38. The DSA investigation reports provided to the ANAO indicate some common reasons for EO and weapons security incidents. These include poor controls at units or depots over EO and weapons handling; lack of adherence to, or poor knowledge of, extant accounting procedures; security breaches including non-compliance with requirements under the DSM; and lack of security awareness or a disregard for some security protocols. The findings of the reports highlight the need for Defence to reinforce, through responsible commanders and managers, the obligations on Defence personnel and contractors to control and secure EO and weapons.

39. Recommendations were made as an outcome of nine of the 24 investigations conducted by the DSA. In these cases, the responsible area was requested to respond to the DSA on any actions taken to implement the recommendations within a specified timeframe, usually within three months after the completion of the investigation report. However, in some cases the responsible area did not respond to the DSA's requests for advice about implementation of recommendations. Strengthened follow-up by the DSA on the implementation of investigation recommendations, including escalation of issues with responsible senior management when appropriate, would better promote timely management action.[23]

Agency response

40. Defence's covering letter in response to the proposed audit report is reproduced at Appendix 1. Defence's response to the proposed audit report is set out below:

> Defence welcomes the ANAO report. Defence has a wide range of security, safety and administrative procedures and policies for the management of explosive ordnance and weapons. Defence acknowledges that there is scope for improvement in the overall management and reporting of explosive ordnance and weapons related security incidents. Defence agrees with the two

[23] See for example, ANAO Audit Report No.25, 2012–13, *Defence's Implementation of Audit Recommendations* which noted that 'once agreed, audit recommendations become a management responsibility, and an effective system to implement recommendations will feature collective ownership within the agency and an action orientation which promotes timely and adequate management activity.' (p. 14).

recommendations made by the ANAO, which will assist with the effectiveness of reporting of explosive ordnance and weapons related security incidents.

Defence takes the security of its weapons, munitions and explosive ordnance very seriously and has a range of measures in place to safeguard them. The effectiveness of the security regime applied to Defence weapons, munitions and explosives is a significant issue for Defence, affecting its reputation, public safety and the public's confidence in Defence's ability to control its equipment.

Defence regularly reviews its policies and procedures on securing and accounting for weapons and munitions, and thoroughly investigates reported loss and/or theft of items either in Australia or overseas.

Recommendations

Recommendation No.1

Paragraph 2.19

To facilitate timely and complete explosive ordnance and weapons security incident reporting, the ANAO recommends that Defence streamline reporting requirements and improve arrangements to coordinate the dissemination of the information reported to relevant Defence stakeholders.

Defence response: *Agreed.*

Recommendation No.2

Paragraph 2.25

To further contribute to Defence's visibility over explosive ordnance security incidents and account for items recovered, the ANAO recommends that Defence establish a formal reporting and acquittal process for explosive ordnance handed in during amnesties.

Defence response: *Agreed.*

Audit Findings

1. Introduction

This chapter provides an overview of explosive ordnance and weapons security incident reporting in Defence. It also introduces the audit, including the audit objective, scope and approach.

Background

1.1 The effective management of explosive ordnance (EO) and weapons is integral to military capability and operations, and contributes to the safety of Australian Defence Force (ADF) members and the public.[24] The Department of Defence (Defence) should appropriately manage and account for its diverse inventory of EO and weapons to ensure these items are readily available for the Australian Defence Force (ADF) when required.

1.2 EO and weapons held by Defence pose potential risks to ADF members and public safety if they are mishandled or fall into the hands of those seeking to misuse them.[25] Other than in specific exceptional circumstances, the sale, resale, transfer, ownership, possession, manufacture and use of many of the EO and weapons held by Defence is illegal in Australia. Many items within Defence's holdings of EO and weapons are strictly controlled under Federal and State laws, and international obligations may also apply.[26] Defence therefore faces unique risks to, and responsibilities for, the security of EO and weapons under its control, and there is a community expectation that those risks will be well managed.

1.3 The management of EO and weapons relies on the design and application of appropriate controls throughout their life cycle, from procurement, storage and handling, through to final use or disposal. A necessary complement to these arrangements is a reliable system for recording

[24] Explosive ordnance (EO) is defined as all munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. Examples include missiles, torpedoes, mines and flares. Defence's definition of EO also includes similar and related non-explosive EO items and components (for example, containers and packaging). The term 'weapon' includes both a 'Defence weapon' and a 'cadet firearm'. See Appendix 2 for Defence's detailed definitions of EO and weapons.

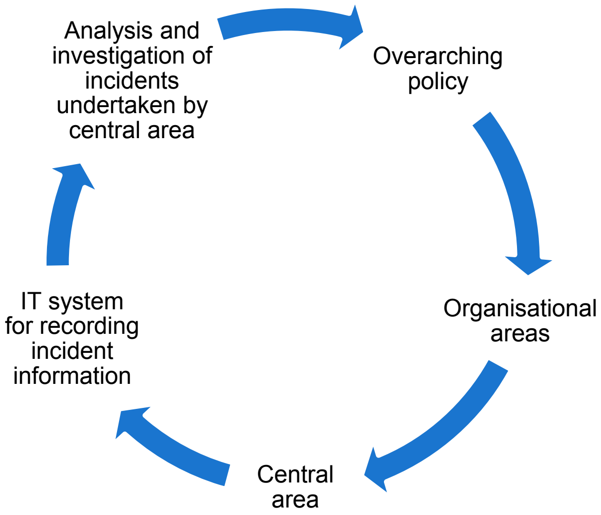
[25] The boundary between the military and civilian spheres can be more porous than is commonly understood. In addition to historical EO and weapons which have found their way into the community over time and continue to be discovered (such as munitions found on old training sites or equipment retained by previous generations of ADF personnel), modern EO and weapons can surface in the wider community as a result of misappropriation, malfunction or loss.

[26] For example, a range of Defence material is provided to Australia subject to end user agreements and other conditions established by the furnishing nation.

and reporting security incidents involving EO and weapons in the event of control failures. Such a system should provide senior management in Defence with visibility of these incidents and their outcomes, and inform the development and application of the procedures used by Defence to store, handle and account for EO and weapons.

1.4 Figure 1.1 illustrates how information from effective incident reporting by areas in an organisation can create a 'feedback loop'. Individual areas in an organisation report incidents to a central area. This central area records the incident information in a centralised IT system. The information is then analysed and further investigated as necessary to develop or adapt overarching policy.

Figure 1.1: Feedback loop of incident reporting


Analysis and investigation of incidents undertaken by central area
Overarching policy
Organisational areas
Central area
IT system for recording incident information

Source: ANAO analysis.

Policy framework for explosive ordnance (EO) and weapons security incidents

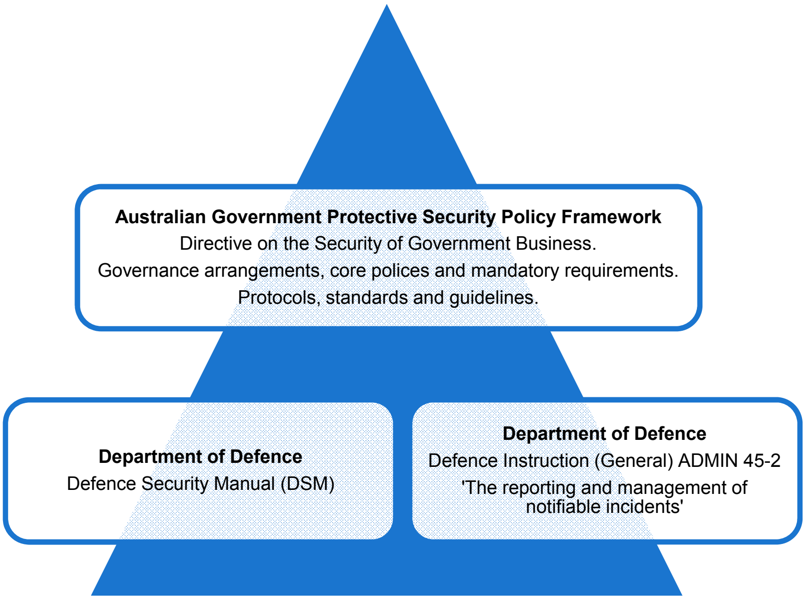
1.5 The high-level policy documents for reporting and investigating EO and weapons security incidents are the:

- Australian Government Protective Security Policy Framework (PSPF);
- Defence Security Manual (DSM); and

- Defence Instruction (General) ADMIN 45-2 'The reporting and management of notifiable incidents'.

1.6 Figure 1.2 illustrates the relationships between the high-level policy documents relevant to EO and weapons security incidents.

Figure 1.2: Defence's policy framework for EO and weapons security incidents


Australian Government Protective Security Policy Framework
Directive on the Security of Government Business.
Governance arrangements, core polices and mandatory requirements.
Protocols, standards and guidelines.
Department of Defence
Defence Security Manual (DSM)
Department of Defence
Defence Instruction (General) ADMIN 45-2
'The reporting and management of notifiable incidents'

Source: ANAO, adapted from Attorney-General's Department and Department of Defence documents.

Australian Government Protective Security Policy Framework

1.7 The Protective Security Policy Framework (PSPF), issued by the Attorney-General's Department, outlines the Australian Government's protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of its people, information and assets, at home and overseas.[27] Under the PSPF, the Government requires agency heads to have in place effective protective security programs that ensure:

- their respective agency's capacity to function;
- the public's confidence in the Government and its agencies;

[27] The Australian Government Protective Security Policy Framework, available from http://www.protectivesecurity.gov.au/pspf/Pages/default.aspx [accessed 2 April 2013].

- official resources and information the Government holds on trust, both from and for the public, and those provided in confidence by other countries, are safeguarded; and
- the safety of those employed to carry out the functions of government and those who are clients of government.

Defence policy and guidance

1.8 Defence policy and guidance is documented in the Defence Security Manual (DSM) and a Defence Instruction. These documents also establish relevant reporting and management processes.

Defence Security Manual

1.9 The DSM is Defence's authoritative protective security policy.[28] The DSM describes the protective security policies, principles, standards and procedures to be followed by Defence personnel and by Defence's contracted external service providers. The DSM defines the following EO and weapons security incidents as major security incidents with consequential reporting requirements:

- Any actual or suspected loss, theft, attempted theft, recovery of, or suspicious incidents involving EO, Defence weapons, associated equipment or cadet firearms.
- The discovery of EO or weapons; actual or attempted break-ins to licensed EO facilities, armouries or weapons storage facilities; and loss, compromise or theft of any keys, cards or other access devices associated with EO and weapons security and storage.
- The inappropriate handling and storage of EO, weapons and associated equipment related to EO and weapons.

1.10 In July 2013, to reduce the administrative burden associated with reporting EO security incidents as major security incidents, Defence amended the requirements in the DSM to remove specific types of EO incidents from the definition of a major security incident. For example, where small arms ammunition is discovered in a container that has been certified as being free

[28] Defence Instruction (General) ADMIN 20-29 Defence Security Manual authorises the DSM as the principal reference for protective security policy within Defence and stipulates that the requirements of the DSM apply to all Defence personnel. As such, the DSM is a lawful and reasonable direction for the purposes of the *Public Service Act 1999* (Cth) and a lawful and general order for the purposes of the *Defence Force Discipline Act 1982* (Cth). The DSM is published in electronic format and therefore is also referred to as the eDSM.

from explosives, under the revised arrangements this is no longer considered a major security incident. The revised policy is discussed further in paragraphs 2.54 to 2.57.

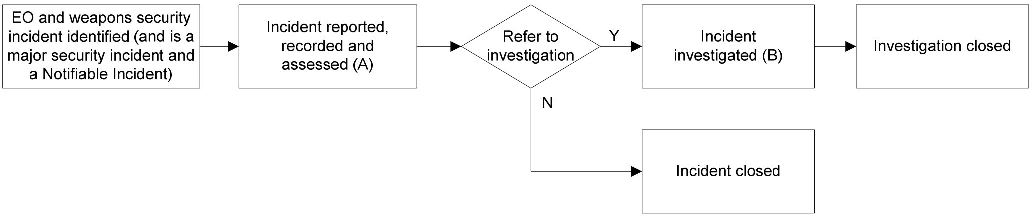
Defence Instruction

1.11 Defence Instruction (General) ADMIN 45-2 'The reporting and management of notifiable incidents' defines a 'Notifiable Incident' and details the mandatory reporting procedures to be followed for these incidents.[29] Under DI(G) ADMIN 45-2, EO and weapons security incidents are one type of Notifiable Incident. Notifiable Incidents must be reported to specific areas within Defence so that appropriate action can be taken.

Defence's process for the reporting and management of EO and weapons security incidents

1.12 Figure 1.3 illustrates the high-level process for the management of EO and weapons security incidents reflected in relevant Defence policy and procedures.

Figure 1.3: Defence's high-level process for the management of EO and weapons security incidents


EO and weapons security incident identified (and is a major security incident and a Notifiable Incident)
Incident reported, recorded and assessed (A)
Refer to investigation
Y
Incident investigated (B)
Investigation closed
N
Incident closed

Source: ANAO analysis of Defence documentation.

Notes:

(A) Assessment of an incident can include any administrative inquiry undertaken by ADF Service units, as well as an assessment of the incident undertaken by the Security Incident Centre in the Defence Security Authority which will then either close the incident, refer it for unit level inquiry or management, or refer it for investigation.

(B) Investigations can only be conducted by qualified investigators acting on behalf of a Defence Investigative Authority. The responsibilities of the six Defence Investigative Authorities in relation to investigations are discussed in Appendix 3.

[29] Department of Defence, Defence Instruction (General) ADMIN 45-2 'The reporting and management of notifiable incidents', March 2010. Under Defence's System of Defence Instructions (SoDI), Defence Instructions (General) (DI(G)) and Chief Executive Instructions operate as the primary policy or directive documents positioned at the highest level of the SoDI framework. DI(G) are issued pursuant to legislation and contain subject matter that applies to all Defence personnel and for which there is a high level of risk for Defence in the event of non-compliance, or where the content may be viewed as sensitive. The Secretary and CDF issue DI(G) jointly, pursuant to section 9a of the *Defence Act 1903* (Cth). The Secretary authorises DI(G) pursuant to powers under the *Public Service Act 1999* (Cth) and they are enforceable pursuant to powers under that Act. The CDF issues DI(G) pursuant to powers under the *Defence Act 1903* (Cth) and they are enforceable pursuant to powers under the *Defence Force Discipline Act 1982* (Cth).

Organisational arrangements

1.13 As a large and dispersed organisation, Defence must have appropriate arrangements in place to provide both local control and effective whole-of-Defence oversight and assurance of the management of EO and weapons. Defence has different lines of reporting and accountability for the management of EO and weapons under the chain of command of each Service, to the Vice Chief of the Defence Force (VCDF)[30], and to the Defence Security Authority (DSA) for security incidents.

1.14 The DSA is led by Defence's Chief Security Officer and is responsible for, among other things:

- setting Defence protective security policy including Defence's primary source of protective security policy, the DSM; and
- monitoring and reporting on Defence's security compliance, performance and risks, including managing the Defence Security Authority Audit Recommendation Management System (dsaARMS) and compiling regular reports on EO and weapons security incidents for the Defence Explosive Ordnance Committee (DEOC).[31,32]

1.15 Defence policy requires that all security incidents, major and minor, be reported to the DSA. The DSA is responsible for: ensuring that reported security incidents have been entered into the Defence Policing and Security Management System (DPSMS); analysing all reported security incidents; and determining the incidents that need to be investigated and the most appropriate Defence Investigation Authority (DIA)[33], Civil Authority or ADF unit to conduct an investigation or administrative inquiry.

[30] Defence refers to the VCDF as being the single point of accountability for EO in Defence.

[31] In addition to these responsibilities, the DSA is responsible for producing security, intelligence and threat assessments, developing and delivering specialist security training, and undertaking personal security vetting for the majority of Commonwealth agencies and related industries. The DSA's funding forms part of Defence's Program 1.5 Intelligence Capabilities. Defence informed the ANAO that the DSA's funding allocation from this program was $52.6 million for 2012–13, is $52.9 million for 2013–14, and is $54.6 million for 2014–15.

[32] The Defence Explosive Ordnance Committee (DEOC) is a senior advisory committee that supports the Vice Chief of the Defence Force (VCDF) as the single point of accountability for the Defence-wide management of EO. The committee is chaired by the Commander of Joint Logistics (CJLOG).

[33] The Security Investigations Unit in the DSA is one of the six DIAs. The other DIAs are the Australian Defence Force Investigative Service (ADFIS); the Service police organisations of the Army, Air Force and Navy; and the Directorate of Investigation and Recovery within the Inspector General Division. The DIAs are authorised by the Secretary and the Chief of the Defence Force (CDF) to conduct formal investigations, including into EO and weapons security incidents.

Recent history of EO and weapons security incidents in Defence

Internal performance audit of weapons munitions and explosives

1.16 In August 2007, Defence completed a comprehensive internal performance audit of its management of weapons, munitions and explosives (WME).[34] The audit findings included:

(a) a concern that neither the management nor the security of WME was fully integrated within Defence;

(b) there was no clear, centralised visibility or single authority with ownership and responsibility for WME throughout their life cycle;

(c) limitations in the systems that account for and monitor WME throughout their life cycle;

(d) limitations in the system for reporting, recording and monitoring security incidents; and difficulty in collating information from a number of different recordkeeping systems which meant that Defence did not have a reliable and comprehensive summary of security incidents involving WME; and

(e) confusing layers of management, processes and accountability that led to uncertainty, and sometimes inaction, with regard to security.

1.17 The audit made 58 recommendations focused on improving Defence's policies and systems for the management and accounting of WME to enhance visibility and control throughout their life cycle. Of particular note, the audit made a number of recommendations to enhance the role and capability of the DSA in the areas of audit, review, compliance and remediation of WME security through changes to policies, procedures and systems. This included developing a WME security compliance, audit and evaluation program to monitor and measure achievement against approved WME security standards;

[34] Department of Defence, 'Security Performance Audit of Weapons Munitions and Explosives', 17 August 2007. This audit was initiated following advice from the Australian Federal Police (AFP) to Defence of a police investigation into the source of a military rocket launcher in the possession of criminal elements, which the AFP believed could have been of ADF origin. A subsequent ADF and AFP investigation confirmed that the weapon was of ADF origin and thought by Defence to have been disposed of some years earlier. In 2008, a serving Army officer received a jail sentence for the theft and sale of the item. The impact of the theft is ongoing as not all of the stolen weapons have been recovered.

and establishing a section within the DSA responsible for policy oversight and compliance management specifically for WME security. The VCDF was given responsibility for implementing the recommendations.

1.18 The objective of the resulting WME Program in Defence was to:

> reduce the exposure of Defence weapons and EO to theft, loss and misdirection through implementation of a comprehensive whole-of-Defence WME security management system that embraces suitable governance, policy, procedural, training, process and people matters as recommended to Government in the WME Security Audit Phase 2 Report.[35]

1.19 In March 2013 Defence informed the ANAO that the department had closed 53 of the 58 recommendations made in the 2007 internal audit. In the same month, Defence's Audit and Fraud Control Division commenced an internal review of Defence's implementation of the WME Program. This review has indicated that work remains for Defence to implement, or demonstrate implementation of, almost half of the 58 recommendations.

Recent EO and weapons security incidents

1.20 Defence recorded 960 EO and weapons security incident reports between 1 January 2011 and 28 August 2013.[36] As part of this audit, the ANAO reviewed Defence data on 693 security incident reports covering the period 1 January 2011 to 25 March 2013. These include publicly reported security incidents on: the recovery of World War II munitions in public areas; the discovery of small arms ammunition and grenades on Defence premises; the discovery of detonators in the pocket of an Army member after being arrested in public by civilian police; the discovery by Australian Customs officials of smoke grenades in the luggage of an ADF member; the loss of a service pistol;

[35] Department of Defence, 'Weapons, Munitions and Explosives Security Performance Audit, Program Initiating Directive', July 2010.

[36] Based on data extracted by Defence from the DPSMS. DPSMS is Defence's primary and approved computer based system used for recording all reports of, and investigations into, major security incidents within Defence. The data extracted has been reviewed and, where necessary, amended by Defence to ensure the data provided to the ANAO accurately reflects all EO and weapons security incidents recorded during the period covered by this audit. In early 2013, Defence commenced a data review and remediation activity to correct the data in DPSMS. This activity and Defence's progress is discussed further in Chapter 3.

The 693 incident reports do not necessarily reflect 693 separate EO and weapons security incidents as DPSMS may have multiple incident records for the same incident, each raised and managed by separate areas within Defence. For example, an EO and weapons security incident may be recorded in DPSMS and assessed and managed by the Army Service Police. The DSA may also choose to raise a separate incident record in DPSMS for the same EO and weapons security incident to enable it to carry out its own assessment and to ensure it has full visibility of the details of the incident.

the theft of pump-action shotguns and handguns from a Navy patrol boat by a serving ADF member; and the loss of a live Claymore antipersonnel weapon.

1.21 Table 1.1 provides a summary of the 693 EO and weapons security incident reports recorded by Defence between 1 January 2011 and 25 March 2013.

Table 1.1: EO and weapons security incident reports recorded in DPSMS, 1 January 2011 to 25 March 2013

Incident Sub-category (A)	2011	2012	1 January 2013 to 25 March 2013	Total
Loss	54	82	9	145
Theft	19	14	7	40
Recovery	116	102	27	245
Incorrect storage/handling	46	112	22	180
Incorrect transport	42	35	6	83
Total	**277**	**345**	**71**	**693**

Source: Department of Defence records of reported EO and weapons security incidents.

Note:

(A) The Defence sub-categories are:

Loss – refers to an incident where an EO or weapon is unable to be found, and is reported as a loss.

Theft – refers to an incident where an EO or weapon is known to have been stolen or suspected of having been stolen and is reported as a theft.

Recovery – refers to an incident when an EO or weapon was not known to be lost or stolen and has been discovered in the public domain or on a Defence site. The most common example is the discovery of World War II munitions on old training ranges or the discovery of EO in containers marked 'free from explosives' (FFE).

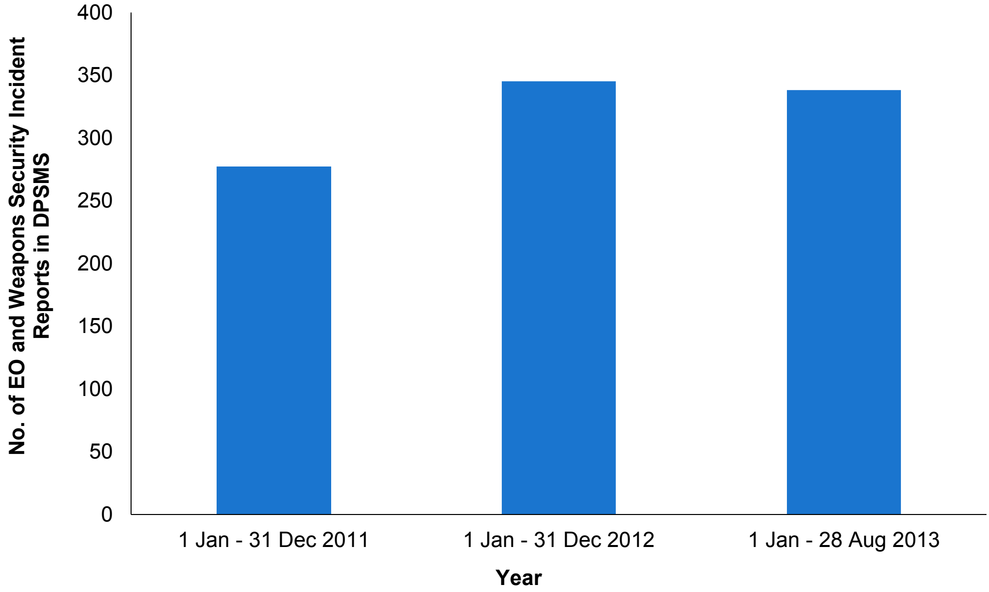
Incorrect storage/handling – refers to an incident that involves an EO or weapon that has not been stored in accordance with Defence requirements. Examples include weapons left on a range or in a Defence staff member's accommodation.

Incorrect transportation – refers to an incident that involves an EO or weapon that has not been transported in accordance with Defence requirements. Examples include EO or weapons transported in an inappropriate vehicle or without the appropriate associated security arrangements in place.

1.22 Defence informed the ANAO that, as at 28 August 2013, Defence had recorded 338 EO and weapons security incident reports for the calendar year commencing 1 January 2013. The composition of the 338 EO and weapons security incident reports recorded during 2013 is: Loss (45); Theft (13); Recovery (200); Incorrect Storage/Handling (52); and Incorrect Transport (28).

1.23 An additional 267 reports have been recorded since 25 March 2013 bringing the total number of EO and weapons security incident reports from 1 January 2011 to 28 August 2013 to 960. As illustrated in Figure 1.4, these additional incident reports represent an increase in the rate of EO and weapons security incident reports during the first eight months of 2013.[37] The ANAO has not examined the additional 267 incident reports recorded since 25 March 2013 as part of this performance audit.

Figure 1.4: EO and weapons security incident reports recorded in DPSMS, 1 January 2011 to 28 August 2013



Source: ANAO analysis of Defence data.

1.24 The following text box describes the multifaceted nature of many EO and weapons security incidents in Defence, and the implications for reporting and management of the incidents.

[37] Defence's view is that the increase does not necessarily reflect an increase in the number of security incidents but may reflect an increase in the number of incidents being reported to the DSA.

The nature of EO and weapons security incidents in Defence

EO and weapons security incidents within Defence can be multifaceted and have a range of implications including, for example, safety or disciplinary. These additional aspects to EO and weapons security incidents can involve a number of areas of Defence, additional policies, procedures, systems and reporting channels. For example, if EO is found in a public area:

1. As a **security** incident, it must be reported through security incident reporting channels.
2. As a **safety** incident, it must be reported to the appropriate area of Defence so that the EO is removed safely.
3. If the incident is also the result of a **suspected theft** from Defence's EO holdings, it must be reported to the appropriate Defence or policing authorities for further assessment and investigation to determine if an offence has been committed[38] and the action, if any, that should be taken.

For the purpose of this audit, the ANAO has focused on Defence's arrangements for monitoring EO and weapons security incidents rather than the other aspects of EO and weapons incidents.

1.25 Between 1 January 2011 and 25 March 2013, Defence initiated 83 investigations into 76 EO and weapons security incidents (approximately 11 per cent of the 693 EO and weapons security incident reports).[39] Twenty-four of these investigations were managed by the DSA's Security Investigations Unit and the remaining 59 were managed by other DIAs. The 83 investigations comprised:

- 24 investigations related to the reported loss of EO and weapons;
- 19 investigations related to the theft of these items;
- 21 investigations related to the recovery of these items; and
- 19 investigations related to the incorrect storage, transport or handling of these items.

1.26 Appendix 4 includes three case studies which discuss some of the more significant EO and weapons security incidents that have occurred in recent years. The case studies demonstrate the integral relationship between effective

[38] Either under the *Defence Force Discipline Act 1982* or under relevant Commonwealth, State or Territory legislation.

[39] These 83 investigations do not relate to 83 separate EO and weapons security incidents. For seven EO and weapons security incidents there were multiple investigations initiated by Defence. Defence informed the ANAO that as at 28 August 2013 an additional 12 security investigations into EO and weapons security incidents had commenced since 25 March 2013. The ANAO did not examine the additional security investigations during the course of this audit.

'upstream' controls of EO and weapons security, and 'downstream' reporting, investigations and analysis which identify and promote responses to issues in the operation of these controls.

Previous ANAO audit reports

1.27 The ANAO completed six performance audits which addressed aspects of Defence's management of EO between 2005–06 and 2012–13.[40] These audits assessed a broad range of issues across the EO life cycle including procurement, contract management, storage and security issues.

1.28 The most relevant of these audits is the ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*, which examined reporting of EO security incidents. The audit found room for improvement in the policies, procedures and systems within Defence for the identification and management of EO security related incidents. Specifically the audit found:

(a) key Defence policy and procedural documents for identifying and managing EO security incidents were inconsistent and confusing; and

(b) there was evidence that not all EO security incidents were being promptly reported to the DSA and that Defence's extant EO security incident reporting had some limitations.

1.29 The ANAO made two recommendations to address the limitations in the guidance, reporting requirements and data for EO security incidents in Defence:

> **Recommendation No.4**
>
> The ANAO recommends that Defence take steps to remove all the inconsistencies in the definitions and requirements for the management of explosive ordnance security incidents in Defence policy and procedural documents.

[40] ANAO Audit Report No.26, 2012–13, *Defence's Remediation of the Lightweight Replacement Torpedo Project,* February 2013; ANAO Audit Report No.40, 2010–11, *Management of the Explosive Ordnance Services Contract*, May 2011; ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy,* April 2011; ANAO Audit Report No.37, 2009–10, *Lightweight Torpedo Replacement*, May 2010; ANAO Audit Report No.24, 2009–10, *Procurement of Explosive Ordnance for the Australian Defence Force*, March 2010; and ANAO Audit Report No.40, 2005–06, *Procurement of Explosive Ordnance for the Australian Defence Force (Army)*, May 2006.

Recommendation No.5

The ANAO recommends that Defence improve its incident reporting and data management of explosive ordnance security incidents.[41]

1.30 Further, ANAO Audit Report No.25, 2012–13, *Defence's Implementation of Audit Recommendations* examined Defence's implementation of ANAO Recommendation Nos. 4 and 5 from Audit Report No.37, 2010–11. The ANAO found that Defence had taken adequate steps to implement Recommendation No.4. However, Defence could not provide the ANAO with sufficient supporting evidence to demonstrate that Recommendation No.5 from the report had been implemented. Defence's progress in implementing Recommendation Nos. 4 and 5 is discussed in Chapters 2 and 3 respectively.

Audit objective, criteria and scope

1.31 The audit objective was to assess the effectiveness of Defence's arrangements for monitoring and reporting EO and weapons security incidents.

1.32 To reach a conclusion against the audit objective, the following high level audit criteria were used:

(a) documentation and advice provided to Defence personnel to assist them in reporting EO and weapons security incidents is adequate;

(b) Defence's reporting arrangements for EO and weapons security incidents are operating effectively (including the processes for Defence personnel to report EO and weapons security incidents, and the process for reporting data on EO and weapons security incidents to the Defence Executive and relevant Defence committees);

(c) Defence's system for recording details of EO and weapons security incidents is adequate; and

(d) the DSA's process for recording, reporting, and responding to the outcomes of investigations into EO and weapons security incidents supports continuous improvement in EO and weapons security incident management.

[41] ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*, April 2011.

1.33 The audit also reviewed Defence's progress, since ANAO Audit Report No.25 2012–13 was tabled in February 2013, in addressing the two recommendations from ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy* referred to in paragraphs 1.29 and 1.30.

1.34 The audit focused on the central administration of EO and weapons security incident reporting in Defence by the DSA and the arrangements in place to assist Defence personnel in reporting incidents. The audit did not seek to assess any ADF Service or unit level arrangements for the management of EO and weapons security incidents (which, under Defence's System of Defence Instructions, are subordinate to the whole-of-Defence requirements that are the main focus of this audit).[42] The audit also did not assess the extent to which all EO and weapons security incidents are reported.

1.35 The audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of approximately $346 000.

Survey distributed to selection of ADF Service Units and EO depots

1.36 As part of the audit fieldwork, the ANAO distributed a survey to a selection of ADF Service units across Army, Air Force and Navy, and to a selection of EO depots. The personnel who received the survey included those whose day-to-day work involved the management of EO or weapons at their unit or depot, and who could potentially be involved in reporting an EO or weapons security incident and any subsequent investigation.[43]

1.37 The survey sought to canvas the opinions of these Defence personnel on the following issues:

- awareness and understanding of EO and weapons security incident reporting procedures;
- ease of following procedures for EO and weapons security incident reporting;
- management support in reporting EO and weapons security incidents;

[42] The audit did not examine controls of EO and weapons, such as Defence's security arrangements for storing or transporting EO or weapons and ADF base security arrangements.

[43] The survey did not include Regional Explosive Ordnance Service offices which, as discussed in more detail in Chapter 2 of this audit report, have been involved in a recent and major breach of Defence's EO security incident reporting requirements.

- EO and weapons security incident investigations; and
- any opportunities for improving the process for EO and weapons security incident reporting.

1.38 The results of the survey are discussed in Chapters 2, 3 and 4 where relevant. The full details and results of the survey are included in Appendix 5.

Report structure

1.39 The remaining chapters broadly follow Defence's process for reporting and managing EO and weapons security incidents:

Chapter Number and Title	Contents
Chapter 2: Reporting EO and Weapons Security Incidents	Examines Defence's processes for reporting EO and weapons security incidents.
Chapter 3: Defence's Information Systems for Recording EO and Weapons Security Incidents and Investigations	Examines Defence's information systems for recording details of all reports of, and investigations into, EO and weapons security incidents.
Chapter 4: EO and Weapons Security Incident Investigations	Outlines Defence's arrangements for the investigation of EO and weapons security incidents. Examines EO and weapons security incident investigation data, monitoring and reporting.

2. Reporting EO and Weapons Security Incidents

This chapter examines Defence's processes for reporting EO and weapons security incidents.

Introduction

2.1 Defence's ability to detect, assess and mitigate security vulnerabilities is dependent upon accurate, timely and consistent reporting of all security incidents across Defence.[44] Defence should have in place clear policies, instructions and procedures for identifying and reporting EO and weapons security incidents, and a reliable information system to manage reported security incidents from initial identification through to the outcome of subsequent investigations.

2.2 Robust reporting frameworks and systems are recognised as important aspects of effective security risk management:

> Incident reporting frameworks can be lead indicators for proactive security measures rather than simply lag indicators of past problems. Near-miss and hazard reporting can be the key drivers of ongoing system improvement rather than the traditional approach, which requires major periodic investments of time and resources immediately following an event.[45]

2.3 As discussed in Chapter 1, Defence's definition of a 'major security incident' includes any actual or suspected: loss, theft, attempted theft, recovery of, suspicious incidents involving, or the inappropriate handling and storage of EO, weapons and associated equipment. Under Defence policy major security incidents are also one category of 'Notifiable Incident'.[46]

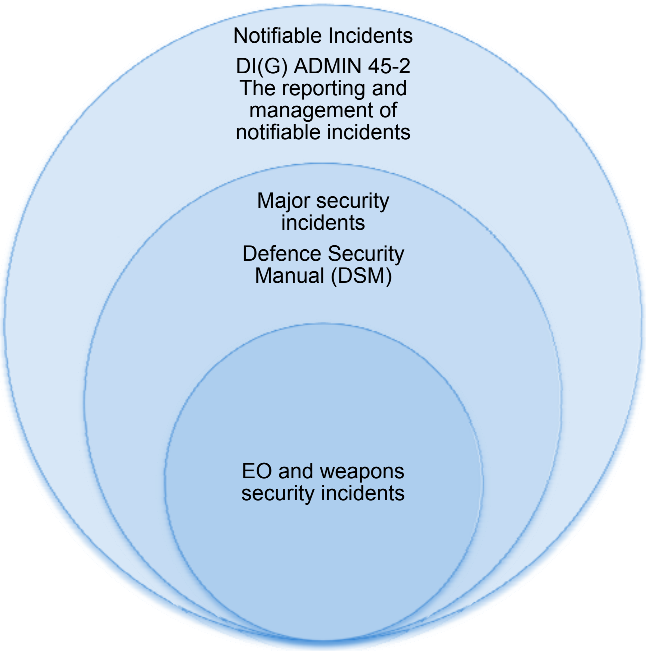
2.4 Figure 2.1 shows that EO and weapons security incidents are a subset of major security incidents which, in turn, are a subset of 'Notifiable Incidents'.

[44] Department of Defence, Defence Security Manual, Part 2:12, Security Incidents and Investigations, Version 4, 7 September 2012, p. 1.

[45] Talbot, J and Jakeman, M, *Security Risk Management*, 2009, pp. 41–42.

[46] DI(G) ADMIN 45-2 'The reporting and management of notifiable incidents' identifies a security incident as one type of 'Notifiable Incident' and defines a security incident as any incident that is not a minor security incident as defined in the Defence Security Manual. Source: DI(G) ADMIN 45-2, 26 March 2010, p. 2 and Annex A, p. 2.

Figure 2.1: Classification of EO and weapons security incidents


Notifiable Incidents
DI(G) ADMIN 45-2 The reporting and management of notifiable incidents
Major security incidents
Defence Security Manual (DSM)
EO and weapons security incidents

Source: ANAO from Department of Defence documents.

2.5 This chapter discusses:

- Defence's reporting requirements for EO and weapons security incidents;
- actual reporting and recording of EO and weapons security incidents;
- a breach of EO and weapons security incident reporting requirements identified by the DSA and advised to the ANAO during this audit;
- Defence's assessment of reported EO and weapons security incidents; and
- recent changes to EO security incident reporting in Defence.

Reporting requirements for EO and weapons security incidents

2.6 As major security incidents and Notifiable Incidents, Defence has developed a number of mandatory reporting requirements for EO and weapons security incidents. The primary sources of these reporting requirements are the DSM and the Defence Instruction (General) DI(G) ADMIN 45-2 'The reporting and management of notifiable incidents'. Some of the reporting requirements in these two policy documents are the same and others differ.[47] The DSM requires Defence personnel and external service providers to report all security incidents in accordance with the instructions given in the DSM. The DSM also states that major security incidents must be handled in accordance with DI(G) ADMIN 45-2.[48] DI(G) ADMIN 45-2 requires Defence personnel to report all suspected Notifiable Incidents (major security incidents are a subset of Notifiable Incidents) to their commander or manager and if the commander or manager determines that the incident is a Notifiable Incident the DI(G) requires the incident be reported immediately in accordance with the instruction.[49]

2.7 Defence's mandatory EO and weapons security incident reporting requirements, as documented in the DSM and DI(G) ADMIN 45-2, are set out in Table 2.1. The table shows that there are a large number of separate EO and weapons security incident reporting requirements. As noted in Chapter 1, many EO and weapons security incidents are multifaceted, and may involve safety, stock control or broader management issues. Table 2.1 includes some reporting requirements associated with these issues.

[47] This was noted in ANAO Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy* which included a recommendation (Recommendation No.4) that Defence take steps to remove all the inconsistencies in the definitions and requirements for the management of explosive ordnance security incidents in Defence policy and procedural documents. While Defence has made some progress in this area, notably through revisions to the DSM, there continue to be some opportunities for Defence to streamline the reporting requirements for EO and weapons security incidents. See paragraphs 2.16 to 2.18.

[48] Department of Defence, Defence Security Manual, Part 2:12, Security Incidents and Investigations, Version 4, 7 September 2012, pp. 2–7.

[49] DI(G) ADMIN 45-2, 26 March 2010, pp. 1–2.

Table 2.1: Mandatory reporting requirements for EO and weapons security incidents in Defence

DSM and/or DI(G) ADMIN 45-2 reporting requirement	Clarification and rationale for requirement
Report to Defence's Security Incident Centre (SIC) within the Defence Security Authority (DSA). • DSM requirement: within 24 hours. • DI(G) ADMIN 45-2: initially by the quickest means, then confirmed in writing. • DI(G) ADMIN 45-2 requires that all security incidents be reported using the XP188 Security Incident Report or direct entry into the Defence Policing and Security Management System (DPSMS). • The DSM mandates the use of the XP188 Security Incident Report form by Security Officers unless a commander or manager has granted a dispensation.[50]	Defence policy requires that all major security incidents be reported to the SIC, which will determine: which security incidents will be subject to investigation by a Defence Investigative Authority (DIA) and the DIA which will conduct the investigation.
Report to the appropriate authority in their Group or Service immediately.	Defence informed the ANAO that the appropriate authority varies depending on which Defence Group or Service the incident occurred within and the nature of the incident (for example, whether the incident is classed solely as a security incident or whether it is also a policing incident). If the incident occurred in an ADF unit then the appropriate authority may be the Provost Marshal for Army, Air Force or Navy.[51]
Report to the local civilian police.[52]	The local police are informed to ensure their awareness of public safety issues and in order to provide investigative support to Defence if required.

[50] A dispensation is the formal acceptance by the appropriate authority that a mandatory DSM requirement cannot be met having considered the justification for non-compliance and accepted the associated risk. Defence informed the ANAO that it did not grant any dispensations between 2011 and mid-2013 regarding the use of the XP188 Security Incident Report.

[51] Provost Marshal (PM) is the title given to the head of each of the three Service Police Organisations: the Navy's Naval Police Coxswain (NPC), the Army's Royal Australian Corps of Military Police (RACMP) and the Air Force's Security Police (SECPOL). In 2006, Defence appointed the first PM ADF in response to a recommendation in the 2005 Senate Foreign Affairs, Defence and Trade References Committee report *The Effectiveness of Australia's Military Justice System.*

[52] This is not a requirement in DI(G) ADMIN 45-2.

DSM and/or DI(G) ADMIN 45-2 reporting requirement	Clarification and rationale for requirement
Report to the Stock Item Owner within 24 hours.[53]	The Stock Item Owner is the manager of the EO and weapons stock involved in the breach. Typically this is the appropriate Support Program Office (SPO) within the Defence Material Organisation such as the Armament SPO for weapons. The stock item owner is informed so that they know that an item of stock is missing and can make amendments/comment on whether the item is written off or remains unaccounted for. In the case of a recovery they can maintain the system and bring the item back onto the appropriate account.
Provide an information copy of the [XP188 Security Incident Report] form to the Group Head or Service Chief and the Chief Security Officer.[54]	An information copy is provided to the relevant Service Chief/Group Head, for their information in case there is a requirement to provide a Ministerial Submission or Hot Issues Brief to the Minister on a particular incident.
Notify the commander or manager of the incident and associated reporting activity, including by providing a copy of the completed XP188 Security Incident Report form.	The chain of command of the person reporting the security incident is informed so they are aware of the incident and can take appropriate action as required. The commanding officer or manager may conduct an initial review (known as a Quick Assessment) into the incident or direct that a routine inquiry be conducted.
Provide a copy of the XP188 Security Incident Report form, for information, to the Australian Defence Force Investigative Service (ADFIS) if the incident involves a suspected offence under the *Defence Force Discipline Act 1982* (Cth) (DFD Act).[55]	ADFIS can become involved in an investigation to determine whether any offences have been committed under the DFD Act and recommend charges if appropriate.
Provide a copy of the XP188, for information, to the relevant ADF Service Provost Marshal.	The relevant ADF Service Provost Marshal is informed so they can investigate from a policing perspective if ADFIS does not investigate the incident.

Source: Based on the DSM, DI(G) ADMIN 45-2 and Defence advice.

2.8 At present, based on the requirements of the DSM and DI(G) ADMIN 45-2, EO and weapons security incidents should be reported to up to

[53] This is not a requirement in DI(G) ADMIN 45-2.

[54] This is not a requirement in DI(G) ADMIN 45-2.

[55] In 2007 Defence created a tri-service authority, the Australian Defence Force Investigative Service (ADFIS), in response to the 2006 *Defence Investigative Capability Audit* which found the need for a tri-service investigative capability.

eight separate stakeholders. While Defence requires use of the XP188 Security Incident Report for reporting to five of the eight stakeholders[56], its policies also provide for a range of other reporting methods, including direct entry into DPSMS, in writing and verbally. These arrangements reflect fragmentation and a general lack of coordination, and highlight scope for Defence to streamline reporting arrangements.

2.9 Under a streamlined reporting approach, the individual seeking to report an EO and weapons security incident would be required to report to a small number of responsible areas, including the chain of command or management, by using a single form or system.[57] Any necessary reporting to other stakeholders should generally be able to be met by drawing on the information reported in the form or system, with consideration given to the most efficient approach to oversee and coordinate the dissemination of information on EO and weapons security incidents. A streamlined approach is more likely to result in EO and weapons security incidents being reported to all relevant stakeholders[58], and an improvement in the DSA's visibility over EO and weapons security incidents, including the number and nature of reported incidents, who incidents were reported to, and when.[59]

Additional reporting requirement for EO security incidents

2.10 In 2011, Defence established the Explosive Ordnance Incident Administration Cell (EOIAC) within Joint Logistics Command (JLC) as the centralised incident cell for the reporting and management of all EO incidents across Defence. The EOIAC was established in order to bring a whole of

[56] Defence advised the ANAO that where an incident is reported via an XP188 as a major security incident, the Defence Policing and Security Management System (DPSMS) automatically generates a copy of the XP188 form for the Security Incident Centre, ADFIS and the relevant Service Provost Marshal.

[57] This is known as a 'report once, use often' approach to reporting, which avoids the need to repeatedly provide the same information.

[58] In June 2013, the DSA informed the ANAO that it was considering options for simplifying EO and weapons security incident reporting. In September 2013, Defence informed the ANAO that the review of current procedures with a view to simplifying them was still underway. Defence did not expect that this work would be completed until towards the end of 2013–14.

[59] As noted in paragraph 1.17, the intended outcome of a number of the recommendations of the 2007 internal performance audit on weapons, munitions and explosives (WME) management was to enhance the role and capability of the DSA, and to establish the DSA as the central point of responsibility for policy oversight and compliance management for WME security. The DSA does not however have full visibility of the extent to which all of the eight mandatory reporting requirements listed in Table 2.1 have been met in each case.

Defence focus to EO incident reporting and management.[60] An EO incident is any incident involving EO that is considered an accident, dangerous occurrence, defect, malfunction, unsatisfactory materiel or an EO security incident.

2.11 Defence EO policy requires that all EO incidents (including EO security incidents) be reported via an Explosive Ordnance Incident form (EO016) to the EOIAC and the appropriate Regional Joint Logistics Unit – EO Services. ADF units are also required to report EO incidents to the appropriate level within Defence through their chain of command.

2.12 The EOIAC currently uses an Excel spreadsheet to record reported EO incidents as an 'interim measure'. The EOIAC does not conduct any analysis or reporting of EO security incidents as this responsibility rests with the DSA.

2.13 As outlined in Table 2.1, Defence policy also requires that EO security incidents be reported to Defence's Security Incident Centre via an XP188 Security Incident Report form. This means that the individual responsible for reporting an EO security incident must complete both the XP188 and EO016 forms and submit each to a different incident centre within Defence. Defence is aware of instances when this has not occurred and only the EO016 was submitted.

2.14 The duplication of reporting requirements and forms for EO security incidents leads to some confusion as to which area of Defence should be notified and which form to use.

Prioritising Notifiable Incidents

2.15 DI(G) ADMIN 45-2 is unclear about how Defence personnel should prioritise the reporting of an incident which may involve multiple Notifiable Incidents. For example, an EO or weapons security incident may also have safety, EO management or disciplinary implications under the DFD Act. From the DSA's perspective, this means that security incidents which have other dimensions may not be communicated to the DSA in the first instance, but only at a later date as related investigations or administrative actions proceed.

[60] The EOIAC was established as part of the broader Explosive Ordnance Incident Reporting and Management (EOIRM) Project. The objective of this project was to address the 'systemic and widespread problems' in the existing Defence EOIRM regime which were largely the result of an 'inefficient, disjointed EOIRM environment'. Source: Department of Defence, 'Business Case, Explosive Ordnance Incident Central Reporting & Management Cell', July 2010, p. 5.

Implementation of Recommendation No.4, ANAO Audit Report No.37, 2010–11

2.16 ANAO Report No. 37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy* noted ambiguities and inconsistencies in Defence's security incident definitions and reporting requirements. These included differences in threshold definitions of EO security incidents, and the consequent threshold requirements for reporting such incidents. The ANAO report noted that ambiguities and inconsistencies within and between the DSM and DI(G) ADMIN 45-2 detracted from their clarity and reduced certainty for those who rely on them for guidance. This affected Defence's ability to effectively oversee and manage these types of incidents. The ANAO recommended that Defence remove all the inconsistencies in the definitions and requirements for the management of EO security incidents in Defence policy and procedural documents (Recommendation No.4).

2.17 Since the 2010–11 ANAO audit, Defence has largely addressed the main ambiguities and inconsistencies in EO security incident definitions and reporting requirements in the DSM and DI(G) ADMIN 45-2 through changes to the definitions and reporting requirements documented in the DSM, to align many of these with those in DI(G) ADMIN 45-2. In February 2013, in ANAO Report No.25, 2012–13, *Defence's Implementation of Audit Recommendations*, the ANAO concluded that Defence's implementation of this recommendation from ANAO Report No. 37, 2010–11 was 'adequate'.[61]

2.18 While the DSM has been amended, the content of DI(G) ADMIN 45-2 has not changed since its last revision in March 2010[62], and there remains scope for Defence to further streamline the requirements in this document and harmonise them with those set out in the revised DSM. Defence's

[61] ANAO Report No.25, 2012–13, *Defence's Implementation of Audit Recommendations* examined the effectiveness of Defence's monitoring of the implementation of ANAO and internal audit recommendations. In reporting the findings from the audit, the ANAO categorised the implementation of recommendations into three groups: adequate—the action taken met the intent of the recommendation, and sufficient evidence was provided to demonstrate the action taken; partial—where the action taken was less extensive than expected by the ANAO (the action either fell short of the intent of the recommendation, or only addressed some of the intended issues), or where Defence may have established a process or procedure to address an issue, however the specific action noted in the recommendation has not been done (this could also be categorised as 'pre-emptive closure'); and insufficient/no evidence—either where there is no indication from evidence or comments that action has been undertaken, or the action taken does not address a recommendation at all.

[62] DI(G) ADMIN 45-2 has also now passed its review date of 30 March 2013. In September 2013, Defence informed the ANAO that it is reviewing a range of issues relating to reporting and management of matters for investigation, and that it has deferred the review of the instruction until there is greater clarity on these issues.

documentation on its process to address ANAO Recommendation No.4 suggests that despite best efforts in some areas of Defence, the fragmented nature of the 'ownership' of Defence policy and procedures continues to challenge Defence's capacity to rationalise and align its requirements for managing and reporting EO and weapons security incidents, and its ability to do so in a timely way.[63]

Recommendation No.1

2.19 To facilitate timely and complete explosive ordnance and weapons security incident reporting, the ANAO recommends that Defence streamline reporting requirements and improve arrangements to coordinate the dissemination of the information reported to relevant Defence stakeholders.

Defence response: *Agreed.*

2.20 *Addressing this issue will compete with other Defence priorities especially with regard to ICT support to reporting, recording and managing EO and weapons security incidents. Therefore it is unlikely this recommendation will be fully addressed in a short timeframe and it is likely to take at least 12 to 24 months to be fully implemented.*

Periodic amnesties for surrender of explosive ordnance not authorised for retention

2.21 Defence Explosive Ordnance Publication 101 (DEOP 101) provides ADF unit managers with the option to declare periodic amnesties on EO held by personnel that is not authorised for retention:

> There are occasions when user units find EO that is not accounted for ... There are also instances when personnel 'acquire', accidentally or otherwise, items of EO during training activities. The continued retention, storage and possible use of the EO obtained under the circumstances described above, will contravene Service regulations and EO handling practices.
>
> Accordingly, in order to discourage the illegal retention of EO for whatever reasons, unit OIC [Officer in Charge] should declare periodic amnesties for unit members to surrender any EO that they are not entitled to hold. Before an amnesty is declared, the unit OIC should seek advice from the local Joint

[63] This challenge primarily relates to Defence's efforts to align the requirements of the DSM (which is 'owned' by the DSA) and the DI(G) (which is 'owned' by the Inspector General Defence).

> Logistics Unit Explosive Ordnance Services staff. EO Services staff is to advise a suitable method to collect, identify and dispose of any EO surrendered.[64]

2.22 The ANAO sought clarification from Defence on how these amnesties are managed in the context of Defence's requirements for EO and weapons security incident reporting. The DSA informed the ANAO that it was not aware of when amnesties occurred, the frequency of amnesties or how they have been managed. Following the ANAO's enquiry, the DSA met with JLC on 20 June 2013 and subsequently advised the ANAO that while amnesties do occur within Defence units, there are no mechanisms in place to centrally track the number of amnesties declared or the types of EO involved.[65] The DSA further informed the ANAO that there are no formal requirements to centrally report EO and weapons recovered through amnesty arrangements. In consequence, there is no process to acquit for items surrendered during an amnesty, and to reconcile Defence-wide records of EO items.

2.23 While acknowledging the potential benefits of local amnesties, the inclusion of this amnesty option in a Defence policy document without careful consideration of the broader consequences for Defence is indicative of a lack of coordination and general fragmentation of Defence's approach to EO and weapons security. It also highlights the challenges Defence must actively address, as a dispersed organisation, to achieve an effective Defence-wide approach to implementing the framework for EO and weapons security.

2.24 On 20 June 2013, in the course of the audit, Defence informed the ANAO that it is working on establishing a formal reporting process for EO amnesties. Defence noted that this may require changes to key policy documents such as the DSM and DEOP 101 and acknowledged that it is important to have the process in place before the return of troops from Afghanistan.[66]

[64] Department of Defence, Defence Explosive Ordnance Publication 101 (DEOP 101), Release 1, July 2011, Regulation 4.4, Procedure 1, Facility Operations - General Instructions, p. 6. DEOP 101 is issued on the authority of the Commander Joint Logistics, who has responsibility to establish EO safety principles and policies for use by all elements of the Australian Defence Organisation. The manual provides those principles and policies as guidance for authorities responsible for all aspects of EO management relating to the storage, transport and handling of EO.

[65] Defence informed the ANAO that these amnesties could be enacted when, for example, units return from exercise or deployment.

[66] This is expected to occur throughout 2013 and 2014.

Recommendation No.2

2.25 To further contribute to Defence's visibility over explosive ordnance security incidents and account for items recovered, the ANAO recommends that Defence establish a formal reporting and acquittal process for explosive ordnance handed in during amnesties.

Defence response: *Agreed.*

Other Defence policies and procedures related to EO and weapons security incidents

2.26 There are also other policies, procedures and guidelines within Defence at the Defence Group, ADF Service and unit levels for the management and reporting of EO and weapons security incidents, with an attendant risk of contributing to fragmentation in Defence-wide arrangements. This audit did not consider these documents in detail. However, during the course of the audit the ANAO found several examples of documents available on Defence's intranet which contained either no reference to Defence-wide reporting requirements for EO and weapons security incidents, or references to out-of-date guidance. If it is considered necessary to have multilayered requirements and guidance in place, then the currency of subsidiary documents should be maintained.

2.27 The range of guidance and resources available to Defence personnel in reporting EO and weapons security incidents is also apparent in the results of the survey the ANAO distributed to selected ADF units and EO depots in May 2013. Respondents indicated that they used up to 10 types of guidance or resources in reporting EO and weapons security incidents.

Reporting and recording EO and weapons security incidents

2.28 Defence policy mandates that EO and weapons security incidents must be reported to the DSA within 24 hours and must be recorded in DPSMS. Specifically, the DSM states:

> DPSMS is the primary and approved corporate computerised system for recording all reports of, and investigations into, major security incidents within Defence. On receipt of a report of a major security incident by a

Defence investigative authority, the incident must be recorded on DPSMS in accordance with extant procedures.[67]

2.29 It is the responsibility of each Defence Investigative Authority (DIA) to log security incidents reported to the DIA onto DPSMS, and to report all major security incidents to the Security Incident Centre through DPSMS. Defence's Chief Security Officer (Head of the DSA) is responsible for: ensuring that reported security incidents have been logged onto DPSMS; analysing all reported security incidents; and determining the security incidents that need to be investigated and the most appropriate DIA, Civil Authority or unit to conduct an investigation or administrative inquiry.

Timeliness of reporting of EO and weapons security incidents

2.30 The ANAO reviewed Defence data on 693 EO and weapons security incident reports recorded in DPSMS between 1 January 2011 and 25 March 2013. The results of the ANAO's analysis are presented in Table 2.2. The results show that the majority of EO and weapons security incidents are not reported within 24 hours as required by Defence policy.

[67] Department of Defence, Defence Security Manual, Part 2:12, Security Incidents and Investigations, Version 4, 7 September 2012, p. 9.

Table 2.2: Comparison of the date an EO or weapons security incident occurred with the date it was reported (DPSMS data for security incidents reported 1 January 2011 to 25 March 2013)

Comparison of date an EO or weapons security incident occurred with the date the incident was reported (based on DPSMS data)	Number (percentage) of EO or weapons security incidents
No security incident occurrence date recorded in DPSMS. [A]	58 (8 per cent)
Date incident occurred is after the date reported (data entry errors)	6 (1 per cent)
Reported on the same day as the incident occurred.	130 (19 per cent)
Reported the day after the incident occurred.	135 (19 per cent)
Reported 2 to 7 days after the incident occurred.	192 (28 per cent)
Reported more than seven days after the incident occurred.[B]	172 (25 per cent)
Total EO and weapons security incidents (1 January 2011 to 25 March 2013)	**693 (100 per cent)**

Source: Department of Defence data.

Note A: The date a security incident occurs is not a mandatory field in DPSMS. As noted in Chapter 1, the date an incident occurs is a key characteristic of an effective incident management system and is a requirement of the PSPF.

Note B: Of these 172 incidents, 116 were reported 8 to 30 days after the incident occurred; 27 were reported 31 to 90 days after the incident occurred; and 29 were reported more than 90 days after the incident occurred (including 5 reported more than one year after the incident occurred.

2.31 Defence provided the following comments in response to the non-compliance with its 24 hour reporting requirement for EO and weapons security incidents:

> The DSA acknowledges and agrees with the level of non compliance. Although the level of non compliance does appear to be significant, the DSA does not have any immediate concerns, and it is confident that security incidents are being appropriately managed by the Units and DIAs. Often the Units will conduct their own search and/or inquiry for missing or lost WME in the attempt to confirm the loss before the security incident is reported and an XP188 raised or entered within DPSMS. The DSA generally does not investigate incidents solely on the timeliness of reporting, only if the incident satisfactorily meets the requirements of an investigation. However, if the DSA (SIC) becomes aware of a significant security incident and there has been a delay in reporting, it would question the reasons for the non-compliance and assess whether an investigation is warranted. The Unit or area would then be educated in the correct reporting timeframe processes. An example of this, is the ongoing DSA investigation into the non compliance of EO [security incidents] … [Discussed in paragraphs 2.43 to 2.53]

> Units are responsible for their own security, however the DSA acknowledges that this needs to be managed in between operational and general duty tasks, thus providing a possible reason for some of the delays.
>
> The timeframes associated with the reporting of security incidents are generally not conducive to a 'just culture'. If the organisation punishes its people for delaying security incident reporting to ascertain the facts in the first instance, then it could induce a culture that may not report all security incidents. The reporting of security incidents does pose a heavy administrative burden on many Units, especially where multiple reporting mechanisms (XP188, EO016, AIMS [Army Incident Management System][68], DPSMS) for an individual incident exist. Maintaining relationships with each of the DIAs and ensuring Defence Units are provided with the correct training and information to report security incidents would be equally valuable as focusing on timeframes.

2.32 Given Defence's view expressed above, the ANAO sought clarification from Defence on the relevance of a mandatory 24 hour reporting requirement when Defence had no expectation that it would be met. Defence informed the ANAO that the mandatory 24 hour reporting requirement is now under review. In the context of that review, it will be important not to lose sight of the benefits of timely reporting.

2.33 The ANAO also analysed the timeliness with which the EO and weapons security incidents were recorded in DPSMS. The results show that the majority of EO and weapons security incidents are recorded in DPSMS within 5 days.

Reporting EO and weapons security incidents to the DSA

2.34 As mentioned in Table 2.1, Defence requires that all EO and weapons security incidents be reported to the Security Incident Centre within the DSA using the XP188 form or via direct entry into DPSMS.[69] This provides for central oversight of these security incidents by the DSA's Security Incident Centre, which is responsible for the assessment, referral and analysis of all major security incidents in Defence. It should also enable the DSA to fulfil its intended assurance role in relation to EO and weapons security.

[68] The Army Incident Management System (AIMS) is mandated for use by Army personnel for recording, managing and creating documentation associated with Notifiable Incidents.

[69] Defence informed the ANAO that in practice the DSA receives initial notification of security incidents through a number of additional means including signal (a form of secure communication used by Defence); the EO016 Explosive Ordnance Incident form; and, on occasion via emails and phone calls.

2.35 However, in practice, many EO and weapons security incidents are not reported to the Security Incident Centre. Defence identified 194 EO and weapons security incidents reported in DPSMS between 1 January 2011 and 25 March 2013, for which primary responsibility rested with a DIA other than the Security Incident Centre. Of these 194 incidents, only 25 (13 per cent) contained information indicating that the DSA carried out some form of initial assessment.[70] Similarly, the DSA has identified 186 EO and weapons security incidents that were not reported to the DSA in accordance with the DSM between January 2011 and March 2013.[71] Consequently, many EO and weapons security incidents are assessed, managed, investigated and/or closed by other DIAs without an initial assessment by the Security Incident Centre, contrary to Defence requirements.

2.36 Additionally, although all EO and weapons security incidents should be reported via an XP188 form, only 40 per cent of respondents to the May 2013 ANAO survey of selected ADF unit and EO depot personnel indicated that they reported EO and weapons security incidents via this method. These survey results show that EO and weapons security incidents may be reported in a variety of ways through a number of reporting channels.

2.37 The ANAO survey also indicated that there is room for improvement in training and awareness for Defence personnel on policies and procedures for reporting EO and weapons security incidents. Fifty nine per cent of respondents recalled having received training on the policies and procedures for EO and weapons security incidents.[72] Additionally, less than half (45 per cent) of respondents either agreed or strongly agreed with the statement that the processes for reporting EO and weapons security incidents have been communicated effectively across the ADF and the department.

2.38 While the Security Incident Centre provides a central point of contact for the reporting and 'triaging'[73] of EO and weapons security incidents, this has

[70] Defence informed the ANAO that it was possible that for some of the remaining 169 incidents there may have been DSA action that was not able to be identified through the DPSMS report, and that to identify these actions would require examination of each incident record in DPSMS.

[71] The DSA has access to security incident records that are created and managed by other DIAs and is therefore able to determine the number of security incidents that are not formally reported to the DSA in accordance with the DSM. Defence identified 186 such EO and weapons security incidents that were created by other DIAs on DPSMS.

[72] In response to the question: 'Have you received any training on procedures and policies for reporting EO and weapons security incidents?'

[73] Triaging relates to the process of assessing incidents to determine the order and priority of their treatment and investigation.

not been supported by reporting and management practices, which continue to involve the control of many security incidents at an ADF Service and Defence Group level. Further, EO and weapons security incidents are not analysed by the DSA with a whole-of-Defence focus to identify their underlying causes which, due to the complex nature of Defence structures and systems, could include: process, behavioural, system and organisational factors.[74] Such analysis is necessary to understand and effectively mitigate risks to Defence's EO and weapons security.

2.39 As noted in Chapter 1, Defence's 2007 internal performance audit of WME made a number of recommendations to enhance the role and capability of the DSA, including through central oversight and assurance of EO and weapons security. The above analysis highlights that Defence has not yet achieved the anticipated level of central oversight and assurance over EO and weapons security through the DSA's Security Incident Centre. In the absence of accurate and complete data on EO and weapons security incidents, it is also difficult for the DSA to effectively fulfil its EO and weapons security policy oversight and compliance management responsibilities. Renewed emphasis is needed for Defence to effectively implement the intent of the recommendations of the 2007 internal performance audit.

Reporting EO and weapons security incident investigations to the Defence executive

2.40 ANAO Report No.37, 2010–11 *Management of Explosive Ordnance Held by the Air Force, Army and Navy* found that there was no regular reporting to Defence senior management on EO and weapons security incidents.

2.41 The DSA now provides regular reports on EO and weapons security incidents to the Defence Explosive Ordnance Committee (DEOC).[75] The reports are developed using DPSMS data and generally provide information on the number of security incidents, and whether the number of incidents is increasing or decreasing. They also describe the circumstances and status of each security incident.

[74] Defence acknowledges this and informed the ANAO that the team responsible for this function was taken offline from September 2011 to April 2013 to support the Australian Government Security Vetting Agency (AGSVA) Data Remediation Project.

[75] The DEOC is a two-star advisory committee that supports the Vice Chief of the Defence Force as the single point of accountability for the Defence-wide management of EO. The committee generally meets three times each year and is chaired by Commander Joint Logistics (CJLOG).

2.42 While these reports include some information on investigations, they tend to focus on the number of investigations underway and closed. There is also little by way of reporting on the results or outcomes of EO and weapons security incidents, nor analysis of underlying trends, possible causes, key risk areas, or proposed remediation activities. Defence informed the ANAO there can be additional reporting or briefings to Defence senior management for individual incidents on a case-by-case basis.

Systemic and multiple breaches of EO and weapons security incident reporting requirements identified by Defence

2.43 On 1 May 2013, during the course of this audit, the DSA identified a number of EO security incidents which had not been reported in accordance with Defence security incident reporting requirements.

2.44 On 30 May 2013, Defence informed the ANAO of the circumstances surrounding this breach of Defence's EO and weapons security incident reporting requirements:

> On 1 May 2013, the DSA Security Incident Centre (SIC) became aware that [a Defence unit] had not been reporting a number of EO related incidents to the DSA. Subsequent inquiries revealed that this [unit] had been involved in approximately 50 EO related incidents since the commencement of 2013, none of which were reported to the DSA via an XP188.[76]
>
> It is alleged that the [unit] had been instructed by [another area in Defence] to not submit XP 188 reports when [the unit] respond[s] to EO related incidents. The DSA believes that this instruction may have been extended to [other units] and may have been in place for some time. The DSA are currently investigating these allegations ...
>
> To date, the [DSA] investigation has determined that 177 EO related incidents were received by the [area in Defence] during the January to March 2013 period ...
>
> The non-reporting of EO related incidents includes the recovery of items from within the public arena. This includes both in-service EO and ordnance that is no longer in-service such as foreign military and World War II EO. The latter can still represent a risk and can have security implications.

[76] As previously discussed, an XP188 is a form for reporting security incidents and is available on the Defence Restricted Network.

> Further evaluation of the unreported EO related incidents by the DSA suggests that some incidents would have warranted further DSA assessment and/or investigation. Failure by the [area in Defence] to formally report the EO related incidents has effectively removed the DSA from this important component of the process.
>
> The DSA is working with [the relevant area in Defence] ... to ensure the procedures for correct reporting of EO incidents will be adhered to. The DSA is aware of the complex nature of current EO reporting requirements that [the unit] and other Defence sections face. An aim of the DSA security investigation will look at the rationale for this reporting and work with relevant stakeholders to determine if this can be rationalised.

2.45 Following an examination of the 177 EO security incidents[77], Defence has determined that 15 were reported via Significant Incident Reports to the Security Incident Centre, and the remaining 162 were reported as EO incidents through other EO reporting channels.[78] Defence confirmed that the 162 EO security incidents were not reported to the DSA as required by Defence security incident reporting requirements. Defence further advised that of the 162 EO security incidents, two met the criteria for a DSA security investigation.[79] Defence also determined that another nine incidents required further DSA assessment, which may lead to a full investigation. The non-reporting of the security incidents to the DSA meant that it could not consider potential security vulnerabilities in a timely way.

2.46 The types of EO involved in these incidents were largely small arms rounds, but also included other in-service, recently out-of-service and obsolete EO including some projectiles, grenades, mortars, flares and fuses. Analysis by the DSA of the EO items involved has determined that a large proportion of the incidents involved EO items that due to their age, condition and/or origin are not of significant consequence to Defence in relation to security vulnerabilities.

2.47 Notwithstanding the DSA's final assessment of security vulnerabilities, discussed in paragraph 2.46, these incidents represent a systemic level of

[77] In most cases the DSA has determined that these Significant Incident Reports were submitted due to circumstances other than in recognition of a security breach. Additionally, the ANAO notes that submission of a Significant Incident Report is not a valid method of reporting security incidents within Defence.

[78] The 177 incidents did not form part of the 960 EO and weapons security incident reports referred to in paragraph 1.20, which covered the period from 1 January 2011 to 28 August 2013.

[79] One of these two incidents involves the discovery of a live in-service grenade by a member of the public in a public area and the other involves the potential theft of items of EO.

non-compliance. Under the current, and mandatory, Defence-wide policy issued by the Secretary and CDF, it is the responsibility of referring areas to report all EO security incidents to the DSA for its consideration of security vulnerabilities.

2.48 The DSA has sought support from the relevant area in Defence to ensure that all EO security incidents are reported in accordance with current security policy, and that the DSA Security Incident Centre receives timely reports on security incidents in accordance with Defence policy.

Underlying causes of the breach of EO security incident reporting requirements

2.49 The DSA commenced an investigation into the alleged non-compliance with Defence security incident reporting requirements in May 2013. The investigation sought to determine the causes, timing and extent of the non-reporting of EO incidents as security incidents. The final investigation report was provided to the relevant ADF Commanders in early December 2013.

2.50 The DSA's investigation findings were that the:

- non-reporting of EO incidents to the DSA was Australia-wide for this particular area of Defence;
- non-reporting of EO incidents to the Security Incident Centre had been happening for a number of years, most likely since 2009 when the requirement to report to the DSA was first implemented through the DSM;
- Defence units involved respond to approximately 700 EO incidents per year—the majority of which should have been identified as major security incidents and reported to the Security Incident Centre—and that almost none of these incidents had been reported to the DSA by the proper channels in accordance with existing policy;
- area of Defence and Defence units involved in the non-reporting appear to have been selective in which Defence policies and procedures they followed in reporting EO incidents and this resulted in non-compliance with security policy; and
- Defence personnel involved made their own assessments on which EO incidents they reported as security incidents to the DSA, despite the DSA being responsible within Defence for assessing the type of incidents that occurred.

2.51 The DSA informed the ANAO on 25 June 2013 that one of the contributing factors to the non-reporting of incidents is that the area involved in the non-reporting is 'faced with an onerous task associated with recovery of EO, which includes the requirement to submit up to five separate reports, depending on the circumstances of an incident'. The breaches of EO and weapons security incident reporting requirements reinforce the benefit to Defence streamlining reporting requirements as discussed in paragraphs 2.8 and 2.9, and reinforcing the accountabilities of Defence personnel and contractors as discussed in paragraph 4.28.

2.52 As a result of the findings from Defence's investigation, the DSA is proposing that Defence undertake a number of policy changes including: re-examining its view of what types of EO incidents should constitute a major security incident that is to be reported to the DSA; identifying simplified reporting mechanisms; revising the DEOP 101 to remove the ambiguity that exists; revising other relevant instructions and EO publications to reference the DSM and clarify EO security incident reporting requirements; and revising the DSM to provide greater clarity on major security incidents that need to be reported to the DSA.

2.53 The detection of this pattern of non-reporting of EO and weapons security incidents was not a result of any compliance or assurance function carried out by Defence. It was identified following an exchange between the DSA and the Defence unit relating to a single incident involving the discovery of items of EO at a private residence. The systemic character of the non-reporting by the Defence units of EO security incidents to the DSA—which was both prolonged and widespread—points to shortcomings in Defence's assurance arrangements pertaining to EO security incident reporting. As part of this audit, Defence was unable to provide evidence of any review, audits or other assurance activity associated with providing some level of assurance to Defence senior management that policies and procedures associated with the reporting and recording of EO and weapons security incidents are being applied across Defence, and are operating as intended. There would be merit in Defence following-up on the initiatives discussed in paragraph 2.52, and any related reform initiatives, through its internal audit function.

Recent changes to EO and weapons security incident policy in Defence

2.54 Under the *Explosives Transport Regulations 2002*, a container or package that has contained Commonwealth explosives, or purports to have contained Commonwealth explosives, must be handled as if it contains explosives unless it has been certified as free from explosives (FFE).[80] The *Explosives Act 1961* imposes penalties for contravention of this regulation. Until July 2013, Defence security policy considered contravention of the FFE regulation an EO and weapons security incident.

2.55 In July 2013, to reduce the administrative burden associated with reporting such incidents as major security incidents, Defence amended the requirements in the DSM to remove specific types of FFE violations[81] related to small arms ammunition from the definition of a major security incident. The revised policy maintains the existing requirement in DEOP 101 Regulation 1.3 to report such incidents to the EOIAC in Joint Logistics Command using the EO016 Explosive Ordnance Incident Report.

2.56 As a result of the change in policy the exempt FFE will not be reported by the DSA as EO and weapons security incidents to senior leaders in Defence, the Defence Explosive Ordnance Committee (DEOC) or other committees. In

[80] Regulation 29 of the *Explosives Transport Regulations 2002*, Statutory Rules 2002 No. 92 as amended made under the *Explosives Act 1961*. The objects of these Regulations are as follows:

(a) to reduce as far as practicable:

(i) the risks of personal injury, property damage and environmental harm arising from the transport of Commonwealth explosives by road or rail; and

(ii) the risk of that transport endangering public safety;

(b) to give effect to the standards, requirements and procedures of the AE [Australian Explosives] Code so far as it applies to the transport of Commonwealth explosives by road or rail;

(c) to establish safeguards for ensuring the security of Commonwealth explosives that are being transported by road or rail.

Other legislative instruments regulate the transport of Commonwealth explosives by civil aircraft or merchant vessels. See the *Air Navigation Act 1920* and the *Civil Aviation Act 1988* and *Navigation Act 2012*.

[81] Under the revised arrangements, FFE violations involving Small Arms Ammunition (SAA) are not considered a major security incident. These incidents are no longer required to be reported to the DSA but are still required to be reported to the EO Incident Administration Cell (EOIAC). FFE violations reported to the EOIAC where 'bulk' or 'large' quantities of live SAA are found in approved EO containers or packaging certified FFE will be escalated to the DSA SIC as a major security incident by the EOIAC via an XP 188 form.

FFE violations involving explosive ordnance other than SAA are considered a major security incident. They must be handled in accordance with DI(G) ADMIN 45-2 'The Reporting and management of Notifiable Incidents'.

February 2013, the Chief Security Officer undertook to review the policy and changed processes after a six month trial period in January 2014.

2.57 The ANAO sought evidence of any risk assessments undertaken by Defence as part of the decision to remove the specific FFE security incidents from the definition of EO and weapons security incidents. In September 2013, Defence informed the ANAO that it did not conduct a formal risk assessment. Defence also informed the ANAO that it held extensive discussions with key stakeholders on the proposed policy change including with JLC and its contractors, and that those discussions addressed potential risks to members of the public, ADF personnel and Defence's reputation.

Conclusion

2.58 Based on Defence-wide policy requirements, EO and weapons security incidents should be reported to up to eight separate stakeholders using a range of methods, reflecting fragmentation and a general lack of coordination in the reporting arrangements. This situation has contributed to non-compliance with individual reporting requirements, and the emergence of coordination issues relating to the notification of Defence stakeholders and investigators. In order to facilitate timely and complete EO and weapons security incident reporting, Defence should streamline reporting requirements and improve arrangements to coordinate the dissemination of the information reported to relevant Defence stakeholders.

2.59 Defence policy mandates the reporting of all EO and weapons security incidents to the DSA to enable the DSA to monitor and triage these incidents. While incident reporting and management generally occurs at an ADF Service and Defence Group level, reporting is often incomplete because there is regular non-compliance with the requirement to inform the DSA about EO and weapons security incidents. For 27 per cent (186 of the 693) of the EO and weapons security incident reports completed across Defence between 1 January 2011 and 25 March 2013, the DSA was not notified in accordance with Defence's reporting requirements. During the course of the audit, Defence identified a further 162 EO security incidents for the period January to March 2013 which had not been recorded as security incidents or reported to the DSA in accordance with Defence requirements.[82] The DSA investigation of the

[82] The 162 incidents were reported as EO incidents through other EO reporting channels to other areas of Defence.

non-reporting of these EO security incidents to the DSA, showed that the non-reporting was widespread, and extended over a more prolonged period, representing a systemic level of non-compliance with the current and mandatory Defence-wide policy issued by the Secretary and CDF.[83] These shortcomings in the reporting of EO and weapons security incidents compromise the integrity of the central monitoring and reporting system and have detracted from the DSA's capacity to fulfil its central monitoring role.

[83] While a DSA investigation into the non-reporting of the security incidents is ongoing, it also indicates that the areas of Defence involved were selective in their application of reporting requirements.

3. Defence's Information Systems for Recording EO and Weapons Security Incidents and Investigations

This chapter examines Defence's information systems for recording details of all reports of, and investigations into, EO and weapons security incidents.

Introduction

3.1 The Australian Government's protective security guidelines highlight the importance of an effective system for recording security incidents:

> Recording security incidents provides valuable insight into an agency's security environment and performance. For instance, multiple minor security incidents could indicate poor security awareness and could alert the agency to the need for increased security training and education. ASAs [Agency Security Advisors] should regularly report details of security incidents and any trends to the agency Security Executive. The statistical information gathered by agencies through security investigations and contact reporting will assist an agency to determine if it requires additional protection and security measures.[84]

3.2 Defence should have a reliable information system to manage reported security incidents from their initial identification through to the outcome of subsequent investigations. An effective security incident recording system captures details of: the time, date and location of the security incident; the type of official resources involved; a description of the circumstances of the incident; a determination of whether the incident was deliberate or accidental; an assessment of the degree of compromise or harm; and a summary of immediate and/or long term action taken.[85]

3.3 A useful information system also enables analysis of the causes of EO and weapons security incidents, and close monitoring of the outcomes of assessments and investigations. Analysis is facilitated by a system which enables users to interrogate data for patterns and trends in the causes of EO and weapons security incidents, and the outcomes of EO and weapons security incident assessments

[84] Attorney-General's Department, Australian Government, Protective security governance guidelines, Reporting incidents and conducting security investigations, 13 September 2011, p. 5.

[85] ibid.

and investigations. Such analysis may provide assurance of the effectiveness of security arrangements, and can identify areas for improvement.

3.4 This chapter examines:

- Defence's primary computerised system for recording all reports of, and investigations into, major security incidents within Defence—the Defence Policing and Security Management System (DPSMS), including:
  - the DSA's review and remediation activity of security incident data in DPSMS; and
  - the extent to which DPSMS supports monitoring of EO and weapons security incidents, assessments and subsequent investigations.
- Other relevant systems used by Defence, including parallel systems for EO and weapons security incident reporting, and the system used to manage recommendations from EO and weapons security incident investigation reports.

Defence Policing and Security Management System (DPSMS)

3.5 DPSMS is a case management tool used by Defence investigators in their reporting, management and investigation of fraud, policing and security matters concerning the Defence Organisation.

3.6 DPSMS is managed by the Inspector General of Defence.[86] The term Policing and Security Organisation (PSO) is used to describe an organisation or group of users within Defence that creates, utilises and administers DPSMS records. These PSOs are the:

- the Defence Security Authority (DSA);
- Australian Defence Force Investigative Service (ADFIS);
- ADF Service Police (Air Force, Army, Navy);
- Inspector General of Defence;

[86] The Inspector General of Defence manages Defence's Fraud Control and Investigations Branch, and is the senior executive responsible for managing Defence's fraud control program which covers the prevention, detection and investigation of fraud, and the recovery of fraudulently acquired money and assets.

- Directorate of Conduct, Performance and Probation;
- Intelligence Security areas incorporating the Australian Signals Directorate[87], the Defence Intelligence Organisation and the Australian Geospatial-Intelligence Organisation;
- Cryptographic Controlling Agency;
- Network Support Agency;
- Joint Logistics Security;
- Defence Science and Technology Organisation (DSTO) Security; and
- Domestic Policing Unit (DPU).

3.7 Defence informed the ANAO that EO and weapons security incident data is generally entered into DPSMS by the DSA's Security Incident Centre following the receipt of a completed XP188 Security Incident Report form from the reporting area of Defence. EO and weapons security incident data may also be directly entered into DPSMS by one of the DIAs on the receipt of other information about a security incident.

History of DPSMS

3.8 Defence identified the need for a centralised investigations case management and reporting system in 1997. DPSMS Stage 1 was implemented in 1999 as an interim solution with limited functionality which did not completely meet PSO requirements. DPSMS Stage 1 was a collection of stand-alone databases maintained by each DIA.

3.9 The DPSMS Stage 2 project commenced in 2002 and was intended to overcome the limitations inherent in Stage 1, by providing Defence with a more powerful centralised case management and reporting system, allowing online access to all data. Defence implemented DPSMS Stage 2 in three phases, or `Builds', as follows:

- Build 1 – February 2008.
- Build 2 – January 2009.[88]
- Build 3 – June 2011.

[87] Previously known at the Defence Signals Directorate.

[88] The extant version of DPSMS during the fieldwork for ANAO Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*, May 2011.

3.10 In August 2010, Defence's Audit Branch completed a Post Implementation Review (PIR) of the DPSMS Stage 2 project. The PIR found that the DPSMS Stage 2 project had fulfilled the original project objectives. However, the estimated cost of the project was $13.7 million compared to the approved budget of $12.6 million and the project was finalised some four years later than planned.[89] Defence finalised a project closure report for this project on 3 April 2013 during the course of this ANAO performance audit.

DPSMS data quality

3.11 As mentioned in paragraph 3.2, an effective security incident information recording system should capture a minimum set of details on security incidents. DPSMS is capable of capturing these details about EO and weapons security incidents through information provided in completed XP188 security incident reports, and subsequent incident assessments and investigations. Notwithstanding system capability, the usefulness of a system for the purpose of analysis remains dependent on the quality of the data entered into the system, and the ability of users to interrogate that data for patterns and trends.

3.12 ANAO Report No. 37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy* examined EO security incident data from 2004 to 2010. The gaps in the pre-2008 data available in DPSMS (that is, DPSMS Stage 1 data) meant that Defence staff had considerable difficulty extracting the relevant data requested by the ANAO relating to losses of EO in Defence.[90] The ANAO's examination of EO security incidents for the period 2008 to early October 2010 found that Defence did not have central visibility of all EO related security incidents through DPSMS. This was largely due to

[89] The estimated cost comprises $12.584 million expended (being the total approved project budget) plus estimated additional project management (staffing) costs estimated by Defence to be $1.14 million. Defence identified contractor failure as the main cause of project delays. Defence also identified that changes to approved requirements and specifications during the life of the project also contributed to cost overruns and delays.

[90] At the time of that audit, Defence informed the ANAO that 'the explosive ordnance security incidents and investigations prior to 2008 were recorded on separate databases maintained by each ADF Service police unit in Defence. These databases were migrated from DPSMS Stage 1 into DPSMS Stage 2 in late 2009. Due to difficulties associated with data migration, some incidents were incorrectly categorised, which means they are not readily identifiable as an explosive ordnance related security incident from the reports provided to the ANAO.' Source: ANAO Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*, p. 112.

incorrect or incomplete data in DPSMS for these incidents.[91] The ANAO recommended that Defence improve its incident reporting and data management for EO security incidents (Recommendation No.5).[92]

3.13 As part of ANAO Report No.25, 2012–13, *Defence's Implementation of Audit Recommendations*, Defence could not provide the ANAO with sufficient supporting evidence that Defence had taken action to address the above recommendation.

3.14 The issue of DPSMS data quality identified by the ANAO was also highlighted in the April 2013 DPSMS Project Closure Report, which noted that the quality of data is sub-optimal. Specifically, the report observed that:

> ... the quality of data could be improved and is very much dependent upon the importance placed on data quality by the stakeholders, as each PSO is responsible for their own records. There is no centralised body with access to all records which has resulted in varying levels of data quality across the application.

3.15 Further, Defence has identified that 'the vast majority of complaints about the capabilities of DPSMS can be traced to problems with poor quality data being entered by users and/or users not utilising the full functionality of the system'.[93]

3.16 The DSA is responsible for providing reports on security incidents to senior management within the Department of Defence. These include the Defence Security Performance Assessment Report (DSPAR) and reporting on EO and weapons security incidents to the Defence Explosive Ordnance Committee (DEOC). The DSA also prepares briefing papers for Defence senior management in preparation for their attendance at Senate Estimates. To provide accurate reports and briefings the DSA has, over the years, manually

[91] This included EO security incidents being incorrectly entered by DPSMS users as incidents other than 'security incidents' resulting in loss of central visibility of these incidents; instances of stolen or lost EO being incorrectly recorded in DPSMS as 'recovered' without ever being reported as being missing; and no central visibility of outcomes of investigations into EO security incidents. See: ANAO Audit Report No.37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy*, pp. 112–113.

[92] At the time of ANAO Audit Report No.37, 2010–11, there was evidence that not all EO security incidents were being promptly reported to the DSA and the extant reporting examined by the ANAO showed some limitations. Defence was not able to provide the ANAO with complete and consistent data on EO security incidents, leading the ANAO to conclude that Defence had yet to achieve visibility of all EO security incidents.

[93] The Inspector General of Defence, in Department of Defence, *Re-thinking systems of inquiry, investigation, review and audit in Defence Stage A report for Secretary and CDF*, August 2012, p. 41.

adjusted DPSMS data outside of the system. Consequently, the security incident data in DPSMS has not always been aligned with the information provided to Defence senior management.

3.17 Defence informed the ANAO that the team responsible for DPSMS data management and reporting was taken offline in September 2011 to support the Australian Government Security Vetting Agency (AGSVA) Data Remediation Project, and the team returned full-time to its usual duties in April 2013. In February 2013, the team began a process of reviewing and correcting selected security incident data in DPSMS.

DPSMS security incident data review and remediation activity, 2013

3.18 The review of DPSMS data by the DSA examined data for security incidents recorded in DPSMS between January 2011 and March 2013. The review encompassed only the DPSMS data fields that have a direct impact on the security incident reporting for which the DSA is responsible.[94] The review did not incorporate a review of all data associated with security incidents in DPSMS.[95] It also did not include other types of incidents (fraud and policing) in DPSMS, which may involve security related matters.

3.19 The initial stage of the review of DPSMS security incident data was completed in March 2013, and covered DPSMS data for security incidents raised in DPSMS from January 2011 to March 2011. The review involved DSA

[94] Specifically, the fields are:

i category (for EO and weapons security incidents this is 'Weapons, Explosives and Controlled Items');

ii sub category (for EO and weapons security incidents these include 'loss', 'theft', 'recovery, and 'incorrect storage/handling' of EO and weapons items;

iii security rating ('major',' minor' or 'reportable major');

iv region (for example, Australian State);

v Defence Group (for example, ADF, Defence Materiel Organisation, Defence Corporate);

vi Defence sub-Group (for example, Army, Navy, Air Force, VCDF); and

vii information security classification (for example, unclassified, protected, secret).

[95] Within DPSMS an incident can be categorised as one of a number of 'types' including, but not limited to:

i Fraud - dishonestly obtaining a benefit, or causing a loss, by deception or other means. As per the definition of fraud in the Defence Fraud Control Plan.

ii. Security - any event that prejudices security or breaches security policy or compliance requirements. Such an event might be deliberate, negligent or accidental and is often the result of a failure to comply with security policy. Source: Defence Security Manual, Part 2:12, Security Incidents and Investigations, Version 4, 7 September 2012, p. 2.

iii. Policing - an incident as categorised in the Australian Standard Offence Categories (ASOC) with the exception of fraud or security related offences.

iv. Other - used to record an error that has been raised and breaches of the Australian Public Service Code of Conduct.

staff generating a report for all incidents categorised in DPSMS as 'security' incidents. This report was then manually cross-checked against the reports that had been previously produced by the DSA outside of DPSMS, in which the DPSMS data had been corrected for reporting purposes. The DSA subsequently developed an electronic method for cross checking and identifying irregularities in data between DPSMS and the reports produced by the DSA outside of DPSMS. This method was used to review the remaining security incidents for the period April 2011 to March 2013.

3.20 As part of the DPSMS data review and remediation activity the DSA identified that 32 per cent of the security incident reports in DPSMS that were reviewed required data correction (5233 from a total of 16 264 security incident reports). Of the 16 264 security incident reports reviewed, 843 were EO and weapons security incident reports. Six hundred and twelve of these incident reports (73 per cent) required some form of data correction. These findings and the significant breaches of EO security incident reporting requirements discussed in paragraphs 2.43 to 2.53 , show that Defence has not yet adequately implemented Recommendation No.5 from ANAO Report No.37, 2010–11, to improve EO security incident reporting and data management.

3.21 Table 3.1 provides a summary of the main errors identified in the EO and weapons security incident data in DPSMS, based on advice provided by the DSA. Most of the errors related to the security rating of EO and weapons security incidents, the security classification of DPSMS incident records and the security classification of WME items. The error rate for EO and weapons security incident data showed no improvement over the January 2011 to March 2013 period.

Table 3.1: Main errors found in EO and weapons security incident data reports in DPSMS

Description of errors identified in review of DPSMS security incident data January 2011 to March 2013 by Defence	Number of EO and weapons security incident reports with data errors[96]
EO and weapons security incidents requiring a change to the incident's security classification (there are two security classification fields related to a security incident—one identifies the security classification of the incident record on DPSMS and the other identifies the classification of the WME item itself. Generally, WME items are not classified).	459
EO and weapons security incidents requiring a change to the incident's security rating from 'minor' to 'major'—noting that all EO and weapons security incidents should have a security rating of 'major'.[97]	181
EO and weapons security incidents requiring a change to the incident's 'sub category', which identifies whether the incident is, for example, a loss, a theft, or a recovery.	147
EO and weapons security incidents requiring a change to the incident's 'sub-Group', which identifies the area of Defence the incident affects. For example, Army, Navy or Air Force.	69
Security incidents recorded in DPSMS categorised as EO and weapons security incidents that should not have been categorised as EO and weapons security incidents.	14
EO and weapons security incidents requiring a change to the incident's security rating from 'reportable major' to 'major'.	10
Security incidents that should have been categorised as EO and weapons security incidents in DPSMS but were not.	7

Source: Department of Defence.

[96] A security incident record may have more than one data error.

[97] The three valid incident security ratings in DPSMS are minor; major; and reportable major. A reportable major incident is an incident involving matters covered by the *Australian Security Intelligence Organisation Act 1979* (Cth) definition of security. The definition of a reportable major incident in the DSM is derived from the Commonwealth Protective Security Manual, which has now been replaced by the Protective Security Policy Framework (PSPF). Under the new PSPF, the definition of reportable major incident is captured by the definition of a major security incident. As noted in Chapter 1, the DSM is yet to be updated to reflect the PSPF.

3.22 Defence informed the ANAO on 14 June 2013 that a total of 931 data corrections were made for EO and weapons security incidents. None were deemed by the DSA to have a potential significant consequence for Defence:

> The DSA assessed the errors identified in the Data Quality Review would not have a potential significant consequence for Defence. The DSA is confident that the identified security incidents would have been assessed and managed appropriately using information contained within the 'quick assessment', XP188, and other relevant documentation.

3.23 Notwithstanding the DSA's assessment of the consequences of the incorrect data, the inaccuracy of many EO and weapons security incident records in relation to the type of incident (for example, loss or theft), and the area of Defence involved, means that the DSA is not able to readily analyse and rely on potentially useful data contained within DPSMS as part of its oversight and assurance function for EO and weapons security. Further, the effort required to correct incorrect DPSMS data is not an efficient use of resources and could be largely avoided through accurate data entry in the first instance.

3.24 After completing its data review in early May 2013, the DSA informed the head of each DIA about the outcomes of the review for the security incident data they 'own' in DPSMS. The DSA provided the DIAs with two options to correct the errors found, either automatically or manually.[98]

Further steps to improve EO and weapons security incident data quality

3.25 Following its DPSMS data quality review, the DSA has undertaken further data quality checks and also intends to institute a standard and regular quality assurance process to check data for all security incidents recorded in DPSMS.[99]

3.26 While strengthening quality assurance of data is a worthwhile activity, consideration should also be given to improving the accuracy of data capture and its input into DPSMS. The overall responsibility for the accuracy of EO and weapons security incident records is shared between reporting areas and

[98] In September 2013, Defence informed the ANAO that three of the DIAs have manually updated their incorrect records in DPSMS and that the remaining incorrect records were sent to the Directorate of Fraud Information Systems in August 2013 to facilitate the automatic update of DPSMS. In December 2013, Defence informed the ANAO that the automatic update is taking longer than initially anticipated due to unforeseen technical problems that are not expected to be resolved until 2014.

[99] In December 2013, Defence informed the ANAO that the quality assurance process is now on hold until the automated update of incorrect security incident data in DPSMS is completed.

the DIAs, including the DSA.[100] As mentioned in paragraph 3.7, EO and weapons security incident data is generally entered into DPSMS by the DSA following the receipt of a completed XP188 form. As a consequence, the accuracy of data may be improved by reducing the discretion available to reporting areas in completing XP188 forms supported by clear guidance and strengthened DSA quality assurance processes.

3.27 The large number of errors in EO and weapons security incident data recorded in DPSMS indicates that Defence personnel responsible for identifying and reporting EO and weapons security incidents experience difficulties in correctly categorising these incidents. The wide range of reporting requirements and methods for EO and weapons security incidents is likely to contribute to reporting errors.

3.28 Introducing mandatory data fields for security incidents, and where practicable, automating data entry for these fields, would assist in improving the quality of the EO and weapons security incident data in DPSMS, and the efficiency of data entry. In addition, Recommendation No.5 from ANAO Report No. 37, 2010–11, *Management of Explosive Ordnance Held by the Air Force, Army and Navy* remains relevant—that Defence improve its incident reporting and data management for EO security incidents. In its response to that recommendation, Defence could also consider reporting and data management for weapons security incidents.

3.29 To help address this set of issues and reduce the number of errors in weapons security incident data, Defence is introducing a business rule to ensure all weapons incidents have a security rating of 'major' on XP188 forms. Defence further advised that this change is significant because all XP188 forms with a security rating of 'major' are directed straight to the Security Incident Centre for consideration.[101]

[100] Sixty-nine percent (424 out of 612) of the EO and weapons security incident reports between January 2011 and March 2013 which had data errors were created in DPSMS by the DSA.

[101] In September 2013, Defence informed the ANAO that:

> Prior to the commencement of the ANAO Audit, the DSA commenced a project to amend the XP188 form to ensure consistent and standard reporting fields. The DSA are working with the IG [Inspector-General's] team [responsible for] managing DPSMS to reduce the number of free text fields and to make the XP188 more user friendly for both the person reporting the security incident and the SIC [Security Incident Centre], to further enhance the management of security incidents.

DPSMS security model for incidents and investigations

3.30 DPSMS holds sensitive and classified information on security, policing and fraud incidents and investigations. The collection, management, handling and release of information recorded in DPSMS is regulated by the *Privacy Act 1988* and the *Freedom of Information Act 1982.* To maintain the confidentiality and integrity of DPSMS data, Defence restricts access to data in DPSMS to authorised DPSMS users using access controls. The controls aim to ensure that only authorised users with a genuine 'need to know' have access to the DPSMS data they need to carry out authorised incident reporting, assessment and investigation duties.

3.31 Access to EO and weapons security incident data within DPSMS is controlled based on the PSO or user group a DPSMS user belongs to, and according to the incident type.[102] Access to data is in the first instance controlled by the PSO user groups or 'silos'. The default position is that users within one PSO user group or 'silo' cannot view records belonging to another user group unless that user has been given access by the administrator for the controlling user group. For example, DPSMS users within the DSA cannot see records belonging to Navy Service Police unless given access by the Navy Service Police DPSMS administrator. Within the PSO 'silos' there are various types of user access levels associated with a DPSMS user's role (such as recorder, investigator, administrator and analyst), which determine the level of access that user has to the incident data within that PSO 'silo'.[103]

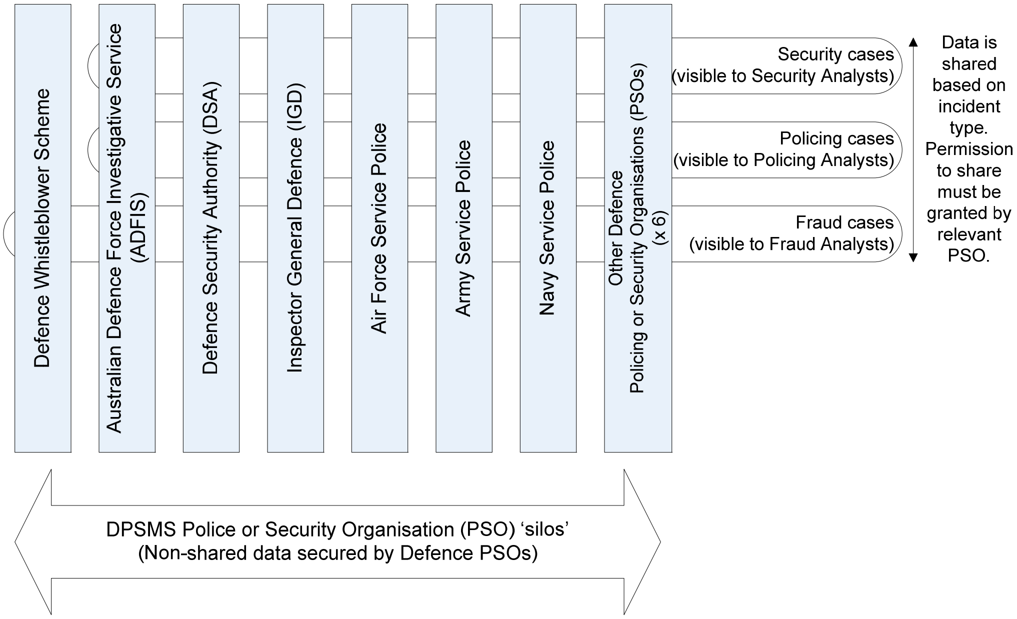
3.32 There are three common incident types in DPSMS – Security, Policing and Fraud. A number of specialist analysts are assigned user accounts which allow them to access a specific incident type across all PSO 'silos' if granted access by each SPO 'silo'. Of particular note, security analysts are able to access all security records in the DPSMS database to enable whole of department security reporting and analysis if they have been granted access by each PSO 'silo'.

3.33 Figure 3.1 provides a high-level overview of the DPSMS data security model, as it relates to access to incident and investigation data across DPSMS 'silos'.

[102] Refer to footnote 95 for an explanation of incident types.

[103] The majority of individual users are defined in DPSMS as either 'investigators' or 'analysts' with the 'analyst' role having read only access to DPSMS data. Some users are both an analyst and investigator and have separate logon identifiers for each role.

Figure 3.1: DPSMS Data Security Model – incidents and investigations



Defence Whistleblower Scheme
Australian Defence Force Investigative Service (ADFIS)
Defence Security Authority (DSA)
Inspector General Defence (IGD)
Air Force Service Police
Army Service Police
Navy Service Police
Other Defence Policing or Security Organisations (PSOs) (x 6)
Security cases (visible to Security Analysts)
Policing cases (visible to Policing Analysts)
Fraud cases (visible to Fraud Analysts)
Data is shared based on incident type. Permission to share must be granted by relevant PSO.
DPSMS Police or Security Organisation (PSO) 'silos' (Non-shared data secured by Defence PSOs)

Source: Adapted from Department of Defence document.

DPSMS user access controls

3.34 The ANAO examined DPSMS data security, focusing on the design and application of key controls. In terms of the design of security controls, Defence generally has relevant policies and procedures in place, including roles and responsibilities in relation to user access management. The design of system security at both the user interface layer and the database layer is also adequate.

3.35 To be effective, security controls must be enforced at an operational level. Through analysis and sample testing, the ANAO noted some limitations in the application of DPSMS security controls. This included lack of documentation relating to user access authorisation; infrequent user access reviews given the large number of users of DPSMS; and no controls around privileged user monitoring and activity.

3.36 A privileged user is able to perform powerful system functions and generally has wider access to systems. According to the Australian Government's Information Security Manual (ISM):

> Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures on systems that lead to cyber security incidents.

> Privileged access allows system-wide changes to be made. An appropriate and effective mechanism to log privileged users will provide greater accountability and auditing capabilities.[104]

3.37 To more effectively manage the risks associated with privileged accounts, the ANAO suggests that Defence monitor and review privileged user activities in DPSMS. This would help to 'ensure that the use of privileged accounts is controlled and auditable'[105] in accordance with the requirements of the ISM.

The DSA's visibility of EO and weapons security incident assessments and outcomes recorded on DPSMS

3.38 Information collected on reported security incidents is valuable in the formulation of policy and procedures, supports security decision making and helps to identify training deficiencies. The knowledge gained from incidents which Defence may consider to be relatively benign and which are not investigated could, when viewed across the whole-of-Defence, provide insights into the health of Defence's EO and weapons management systems.

3.39 The outcomes of assessments, inquiries and other actions taken in response to EO and weapons security incidents which are closed without investigation are held in a number of different fields and attachments within DPSMS. This information is not easily accessible or available for analysis. Defence informed the ANAO in September 2013 that:

> Any information that is entered into an assessment note or into the running sheet note as an incident description can be extracted as a report from DPSMS, enabling analysis of outcomes and other actions undertaken for each incident. ... Where the information is only available in an attachment, this information requires manual extraction to enable the analysis of assessments, outcomes and other actions undertaken. The manual extraction has resource implications.

3.40 The ANAO suggests that Defence consider the use of 'closure codes' in DPSMS to indicate the outcome of assessments of EO and weapons security incidents which do not progress to investigation. These codes could provide a simple reference system on the outcomes of EO and weapons security incident

[104] Department of Defence Intelligence and Security, *Australian Government Information Security Manual: Controls*, April 2013, p. 192.

[105] ibid, p. 193.

assessments and therefore enable a Defence-wide view of the causes of these incidents.

3.41 An example of 'closure codes' can be found in the United Nations' International Ammunition Technical Guidelines.[106] The guidelines provide an example system of cause and closure codes which investigating authorities can use to analyse the results of investigations or assessments of incidents involving ammunition. More than one cause or closure code can be attached to an incident and the code can be modified as further information becomes available.

The DSA's visibility of EO and weapons security incident investigations recorded on DPSMS

3.42 A limited number of DSA staff have access to all security incidents and investigations for the purpose of high-level reporting to Defence Committees and senior management. However, these DSA staff do not use DPSMS to monitor investigations undertaken by other DIAs. The DSA informed the ANAO that if it requires further information on a specific EO and weapons security investigation undertaken by one of the other DIAs, it requests the DIA to provide this information rather than access the relevant details using DPSMS.

3.43 The DSA's limited access in viewing all EO and weapons security investigation records on DPSMS means that the DSA, as the central point of contact for security incidents, does not have a Defence-wide view of actions undertaken and the status of investigations. This poses a challenge to the DSA when attempting to follow-up on investigations, particularly when the respective DIAs and ADF Service Units have not provided feedback or an update on cases being investigated. It also impacts on the DSA's ability to analyse and respond to emerging EO and weapons security issues for Defence.

3.44 During the audit, the DSA noted that it was in negotiation with the other DIAs to increase the number of DSA analysts with access to all DPSMS security incident data. These negotiations have not progressed to date, notwithstanding the DSA's central authority in this area.

[106] See United Nations Office for Disarmament Affairs – International Ammunition Technical Guidelines: 11.20 Ammunition Accidents, Reporting and Investigation – Ammunition Accident Investigation Methodology, Annex C: Example Cause and Closure Codes, http://www.un.org/disarmament/convarms/Ammunition/IATG/docs/IATG11.20.pdf [Accessed 18 July 2013].

Other information systems used in Defence to maintain records of EO and weapons security incidents and investigations

Defence Security Authority Audit Recommendation Management System

3.45 The Defence Security Authority Audit Recommendation Management System (dsaARMS) is a database used by the DSA for recording and tracking recommendations, including recommendations from all EO and weapons security incident investigation reports (across the DIAs). The purpose of dsaARMS is to enable the DSA to monitor and follow-up on the progress of implementation of recommendations by the responsible area in Defence.

3.46 In September 2011, the DSA's reporting team was taken offline for some 18 months to work on another major remediation project.[107] As a result, dsaARMS was not used to monitor the implementation of recommendations from EO and weapons security incident investigation reports from September 2011 to the end of March 2013.

3.47 Defence informed the ANAO in May 2013 that:

> Since coming back online, dsaARMS has been updated with the information that was available to the DSPR [Directorate Security Performance Review of the DSA] and outstanding recommendations/actions are being updated as they are received by the team. The system will be used as updates are received and internal DSA processes need to be reviewed to ensure that dsaARMS is being used.

Other information systems for EO and weapons security incident records

3.48 In addition to DPSMS, there are other electronic information systems in use within the Defence organisation which also contain data on WME incidents (including EO and weapons security incidents). For example, the Army Incident Management System (AIMS) is mandated for use by Army personnel for recording, managing and creating documentation associated with Notifiable Incidents.

[107] See paragraph 3.17 .

3.49 As discussed in Chapter 2, the Explosive Ordnance Incident Administration Cell (EOIAC) collects information on EO incidents (including EO security incidents) through the receipt of EO incident forms and records the data on a spreadsheet. The EOIAC does not conduct any analysis or reporting of EO security incidents as this responsibility rests with the DSA.[108]

3.50 The duplication of information systems for maintaining records of EO security incidents has some disadvantages. These include: reliance on manual checking and communications between the EOIAC and the DSA to align their records and the absence of a link between the EOIAC's spreadsheet and DPSMS.[109]

3.51 The continued use of multiple information systems for recording EO and weapons security incidents contributes to fragmentation within Defence and has the potential to undermine Defence's efforts to achieve central visibility of EO and weapons security incidents, and consequently the effectiveness of the department's monitoring and management of the risks associated with EO and weapons security incidents. The recent discovery of 162 EO security incidents that were not reported in accordance with Defence security incident reporting requirements is an example of risks relating to the fragmentation of Defence systems and processes coming to fruition.[110]

Conclusion

3.52 DPSMS is the primary and approved electronic system for recording all reports of, and investigations into, major security incidents within Defence. In the context of a reporting framework which involves various Defence Investigative Authorities (DIAs) entering data into DPSMS based on information provided by reporting areas, there is a shared responsibility to enter data accurately, and a central responsibility to periodically test the integrity of that data. The DSA has sought to address DPSMS data quality issues through a review of all security data in DPSMS from the period January 2011 to March 2013. Of the EO and weapons security incidents examined as part of this review, 73 per cent required some form of data correction; reflecting ongoing issues around the efficiency and effectiveness of data entry. These findings and the significant breaches of EO security incident reporting

[108] The EOIAC and its role in EO and weapons security incident reporting was discussed in Chapter 2.

[109] There are informal information sharing arrangements between the EOIAC and the DSA.

[110] This was discussed in Chapter 2.

requirements discussed in Chapter 2, show that Defence has not yet adequately implemented Recommendation No.5 from ANAO Report No.37, 2010–11, to improve EO security incident reporting and data management. Following its DPSMS data quality review, the DSA intends to institute a standard and regular quality assurance process to check data for all security incidents recorded in DPSMS. Introducing mandatory reporting data fields, and where practicable, automating data entry for these fields, would also assist in improving the quality of the EO and weapons security data in DPSMS, and the efficiency of data entry.

4. EO and Weapons Security Incident Investigations

This chapter outlines Defence's arrangements for the investigation of EO and weapons security incidents. It also examines EO and weapons security incident investigation data, monitoring and reporting.

Introduction

4.1 Defence conducts an extensive range of inquiries, investigations and reviews. These activities address fraud, personnel disputes or conflicts, criminal misconduct, operational or equipment incidents, staffing or performance issues, safety incidents and security incidents.

4.2 Investigations in Defence are conducted to either a criminal standard or an administrative standard. Criminal standard investigations[111] are conducted within Defence by the Defence Investigative Authorities (DIAs). These are the Australian Defence Force Investigative Service (ADFIS), the Service police organisations of the Army, Air Force and Navy, the DSA and the Directorate of Investigation and Recovery within the Inspector General Division.[112]

4.3 During the period from 1 January 2011 to 25 March 2013, there were 83 investigations [113] of EO and weapons security incidents recorded in DPSMS.[114] As noted in Chapter 1, the 83 investigations related to security incidents in four categories: the reported loss of WME; the reported theft of

[111] These investigations are primarily to ascertain whether offences have been committed and are part of a broader criminal justice, civil penalty or military discipline system. Their conduct is based on a criminal law investigative model. Evidence gathered as part of investigations into offences can be used in adversarial proceedings before civilian courts and service tribunals where guilt must be proven beyond reasonable doubt.

[112] The legislative authority of ADFIS and the Service police is contained within the *Defence Force Discipline Act 1982*. In contrast, non-ADF DIA investigators (including the Inspector General and the DSA) have no legislative authority. However, when performing investigative functions on behalf of the Commonwealth, they must comply with relevant Commonwealth, State and Territory legislation including, but not limited to, the *Crimes Act 1914* (Cth), the *Evidence Act 1995* (Cth), and the *Criminal Code Act 1995* (Cth). The role of each of the DIAs is outlined in Table 4.1.

[113] These 83 investigations do not relate to 83 separate EO and weapons security incidents. For seven EO and weapons security incidents there were multiple investigations.

[114] These incidents were investigated by one of the DIAs, with ADFIS or the DSA being the primary investigator in the majority of the incidents (ADFIS was the primary investigator in 27 investigations and the DSA was the primary case officer in 24 investigations).

WME; the reported recovery of WME; and the reported incorrect storage, transport or handling of WME items.[115]

4.4 This chapter examines:

- the arrangements for conducting EO and weapons security investigations in Defence; and
- ANAO analysis of the available records in DPSMS for a sample of 24 EO and weapons security incident investigations undertaken by the DSA during the period from 1 January 2011 to 25 March 2013.

Arrangements for conducting EO and weapons security investigations within Defence

4.5 The following sections of the report detail the governance and organisational arrangements for conducting EO and weapons security investigations within Defence, including the relevant policies, and roles and responsibilities.

Australian Government frameworks and standards

4.6 The Australian Government Protective Security Policy Framework (PSPF) outlines the requirement for Australian Government agencies to undertake a security investigation for each security incident that 'has, or could have, compromised the Australian Government.'[116] Under the PSPF, agencies must have in place procedures for reporting and investigating security incidents, and take appropriate corrective action.[117]

4.7 The Australian Government Investigations Standards (AGIS) provide the minimum standard for agencies conducting investigations relating to the legislation and programs they administer. The AGIS is mandatory for all agencies subject to the *Financial Management and Accountability Act 1997*.

[115] Defence informed the ANAO that between 25 March 2013 and 28 August 2013 an additional 12 EO and weapons security investigations had commenced. The ANAO did not examine these additional EO and weapons security investigations during the course of this audit.

[116] *Australian Government Protective Security Policy Framework*, p. 15.

[117] In accordance with the provisions of the Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations, and the Australian Government Investigations Standards. *Australian Government Protective Security Policy Framework*, p. 15.

Defence-wide manuals, standards and instructions

4.8 The Defence Security Manual (DSM) outlines the requirements for all investigations of security incidents in Defence. The DSM states that:

> Defence will ensure that all security incidents are properly reported and that allegations regarding the security incidents are investigated and dealt with in accordance with the relevant policies and legislation, and the Australian Government requirements in the PSM[118] and ISM.[119]

4.9 The DSM makes clear that the DSA has a central role in determining whether a security incident requires investigation, and who should take carriage of the investigation. The DSM states that the DSA Security Incident Centre 'will determine which incidents will be subject to further formal investigation.' The DSM also states that the Chief Security Officer is responsible for 'determining the most appropriate Defence investigative authority, Civil Authority or unit to conduct an investigation or administrative inquiry in the event of a major security incident.' The DSA must also be advised of the outcome of investigations and assign any recommendations for implementation to the relevant area of Defence.[120]

4.10 The Defence Investigation Standards, published in June 2009, provide all DIAs with minimum standards for investigations of offences under the *Defence Force Discipline Act 1982*, and, where applicable, other Commonwealth,

[118] The PSM refers to the *Protective Security Manual*. Under the PSM agencies were required to ensure that allegations regarding security incidents were dealt with in accordance with relevant legislation, including the *Freedom of Information Act 1982*, the *Ombudsman Act 1976*, the *Crimes Act 1914,* the *Criminal Code Act 1995,* the *Australian Security Intelligence Organisation Act 1979*, the *Privacy Act 1988*, and any other relevant government policy, agency direction or instruction. Source: *Protective Security Manual*, Part G, paragraph 4.13. The PSM has now been superseded by the PSPF.

[119] The ISM refers to the Australian Government Information Security Manual. This manual is the standard which governs the security of government Information Communication Technology systems. It complements the PSPF.

[120] The DSM states that:

> At the completion of an investigation into a security incident, the Defence investigative authority **must** provide the CSO [Chief Security Officer] with an investigation report detailing actions undertaken throughout the course of the investigation, the findings of the investigation and any remedial recommendations.

Further the DSM states that:

> The CSO will ensure that recommendations from the investigation are assigned for implementation to all areas of Defence affected by the recommendations.
>
> Group Heads and Service Chiefs **must** assign an officer at or above the SES Band 1 / 07 level to be responsible for implementing the investigation's recommendations. The appointed officer **must** report back to the CSO on action taken in response to the recommendation within three months of the investigation report, or other timeframe specified by the CSO.

Department of Defence, Defence Security Manual, Part 2:12, Security Incidents and Investigations, Version 4, 7 September 2012, p. 9.

State and Territory legislation. They also provide the minimal standards for the development of detailed operating procedures and instructional guidance.

4.11 There are also a number of Defence Instructions (General) (DI(G)s) which are relevant to investigations of incidents within Defence. These DI(G)s include DI(G) ADMIN 45-2 'The reporting and management of notifiable incidents' which notes the roles of the DIAs in conducting investigations[121], DI(G) ADMIN 45-4 'Defence Investigations Standards' which authorises the Defence Investigation Standards, and DI(G) ADMIN 67-2 'Quick assessments' which provides guidance to commanders and supervisors on the procedures for conducting a Quick Assessment (QA) of an incident.

Organisational arrangements – conducting investigations in Defence

4.12 As noted in paragraph 4.2, there are six DIAs. They are the only bodies within Defence authorised by the Secretary and the Chief of the Defence Force (CDF) to conduct formal investigations. Each of the DIAs can be involved in the investigation of a security incident. However, as noted in the DSM, the DSA is the central group responsible for the overall management of security incidents in Defence. Investigations can only be conducted by suitably qualified investigators acting on behalf of a DIA. The table below outlines the DIAs and their roles and responsibilities in relation to security incident investigations.

[121] As defined in Chapter 1, certain incidents involving Defence and its resources are known in Defence as 'Notifiable Incidents'. These types of incidents must be reported to specific areas within Defence so that appropriate action may be taken. An EO and weapons security incident is one type of 'Notifiable Incident'. Defence Instruction (General) ADMIN 45-2 'The reporting and management of notifiable incidents' defines a 'Notifiable Incident' and details the mandatory reporting procedures to be followed.

Table 4.1: Responsibilities of Defence Investigative Authorities – security incident investigations

Defence Investigative Authority (DIA)	Roles and responsibilities in relation to security incident investigations in Defence
Defence Security Authority (DSA)	The primary areas in the DSA involved in investigations of security incidents within Defence are: • The Security Incident Centre, which assesses, refers and analyses security incidents. • The Directorate of Security Intelligence and Investigations, which conducts investigations into suspected security incidents within Defence. • The Security Investigations Unit, which investigates major security incidents that may be in breach of the DSM and its referenced authoritative texts, or any relevant legislation as directed by the Chief Security Officer; and examines serious and complex security incidents which may significantly damage Defence capability or its reputation, such as incidents concerning weapons, munitions and explosives.
Australian Defence Force Investigative Service (ADFIS)	ADFIS is a tri-service unit responsible for complex and major investigations involving the ADF, which is led by the Provost Marshal ADF. The role of ADFIS is to assist the Chief of the Defence Force and the Service Chiefs to maintain discipline in the ADF through the lawful, ethical and effective investigation of matters involving persons subject to the jurisdiction of the *Defence Force Discipline Act 1982*. While ADFIS is not mandated to investigate security incidents, security incidents can be referred to ADFIS if they potentially contain a criminal element, and/or discipline offences.
Inspector General Division	The Directorate of Investigation and Recovery within the Inspector General Division conducts investigations into matters such as alleged fraud, serious misconduct, commercial impropriety, corrupt practices and conflicts of interest. The Inspector General also manages the Defence Whistleblower Scheme and DPSMS.
Single-Service Policing organisations (Army, Navy, Air Force)	The Army, Air Force and Navy each have their own Service police. As DIAs, the Single-Service Policing organisations are authorised and required to conduct independent investigations (where they have jurisdiction), unfettered by the chain of command or line management, into suspected major security incidents in accordance with DI(G) ADMIN 45-2. The Single-Service Police are responsible for assisting Service Chiefs with the maintenance of discipline and investigation of minor criminal or discipline matters.

Source: Defence documentation.

4.13 In addition to the investigation of EO and weapons security incidents by the DIAs, ADF Service units may conduct their own administrative investigation, inquiry or review of an EO and weapons security incident. However, these activities are not subject to the same legislative and governance framework as DIA investigations.[122] Further, the outcomes of administrative investigations, inquiries or reviews of EO and weapons security incidents undertaken by ADF Service Units are not always recorded on DPSMS.

4.14 In summary, Defence's internal arrangements can give rise to multiple investigations of a single EO and weapons security incident. As discussed in paragraph 4.24, one in four of the DSA investigations examined by the ANAO was subject to a parallel investigation by another DIA and/or administrative inquiry by the relevant Service unit.

The DSA's procedures for recording and monitoring investigations of EO and weapons security incidents

4.15 The Security Incident Centre's and Security Investigation Unit's Standard Operating Procedures provide guidance on assessing security incidents, conducting investigations into security incidents, recording the results of those investigations, and monitoring and follow-up actions. The following paragraphs focus on the requirements the DSA is to meet under these Standard Operating Procedures.

4.16 In an investigation of a security incident, the DSA's investigators are required to use Defence systems to record the results—primarily DPSMS, but also other approved Defence records management systems including Objective[123] and the Electronic Document Management System (eDMS).[124]

[122] Annex B to the *Re-thinking systems of inquiry, investigation, review and audit in Defence* provides the following information on inquiry mechanisms within Defence:

> The term 'inquiry' in Defence is used to describe fact-finding processes that inform administrative and command decisions, including decisions to prevent recurrence of an incident, to change systemic problems, or to refer an individual for investigation. While individuals may ultimately be criticised in an inquiry report, the purpose of the inquiry is not to determine whether individuals are liable to criminal or disciplinary sanctions. However, an administrative inquiry may result in an individual being referred for a disciplinary or criminal investigation or used as the basis for decisions regarding the imposition of administrative sanctions or other management action.
>
> Many inquiries in Defence are not conducted in accordance with formal procedures laid out in whole-of-government or Defence-specific legislation or policy.

Department of Defence, *Re-thinking systems of inquiry, investigation, review and audit in Defence: Stage A report for the Secretary and CDF*, Annex B: Legal Framework Analysis, p. 4.

[123] Objective is Defence's primary document management system on the Defence Restricted Network.

4.17 The DSA's investigators aim to complete an investigation within a 90 day period. If an investigation cannot be concluded within this timeframe, the head of the Security Investigations Unit must be advised and consultation should take place to determine the future direction of the investigation.

4.18 Investigation reports should usually contain the reasons for the report including details of the incident; details of the individuals interviewed and information obtained as part of the investigation; an assessment of the incident; a conclusion as to why the incident occurred; and recommendations to prevent similar incidents occurring, including any actions against the person(s) responsible for causing the incident.[125] This is discussed further in the following major section of the report, which discusses the ANAO's analysis of a sample of the DSA's investigations of EO and weapons security incidents.

ANAO analysis of available records for a sample of DSA investigations of EO and weapons security incidents

4.19 As part of this audit, the audit team examined records of 24 investigations of EO and weapons security incidents undertaken by the DSA from 1 January 2011 to 25 March 2013. During this period, there were 83 security investigations involving the loss, theft or recovery of EO and weapons across Defence. Of these 83 investigations, the DSA SIU was the primary case officer in 24 cases (29 per cent). Of these 24 investigations:

- 13 were conducted in 2011, and all of these investigations are now closed;
- seven were conducted in 2012, with five closed and one ongoing as of 25 March 2013; and
- four were conducted in 2013, with all four ongoing as of 25 March 2013.

4.20 Table 4.2 lists the Group or Service which originally reported the 24 EO and weapons security incidents investigated by the DSA.

[124] The eDMS is Defence's primary document management system on the Defence Secret Network.

[125] Not all of the DSA's investigations result in an investigation report. There is no requirement for an investigation report to be developed for every DSA investigation.

Table 4.2: Number of EO and weapons security investigations undertaken by the DSA, based on originating Group or Service, 1 January 2011 to 25 March 2013

Group or Service	No. of EO and weapons security investigations originating in Group or Service
Vice Chief of the Defence Force (VCDF)	6
Army	6
Air Force	4
Navy	2
Other	6

Source: ANAO analysis of Defence documentation.

Note: 'Other' includes security investigations involving contractors responsible for storing or transporting Defence weapons or explosive ordnance.

Conducting investigations

4.21 For the 24 DSA investigations examined by the ANAO, the reasons to initiate the investigation included that: the EO or weapon reported lost or stolen represented a significant risk to the community; there was a suspected level of criminality in the EO and weapons security incident; and there had been previous EO and weapons security incidents involving the unit or contractor. For most of the investigations, the reason for initiating the investigation had been recorded in DPSMS as part of the investigation record.

4.22 In accordance with the DSA's Standard Operating Procedures, there were notes and records in DPSMS for all of the investigations. The DPSMS contained relevant documents, such as records of telephone conversations and email correspondence with persons of interest, records of site visits and photographs of evidence. Defence informed the ANAO that additional evidence for investigations is also documented on other Defence record management systems such as Objective, and the eDMS.[126]

4.23 The investigation records in DPSMS also indicated that DSA investigators worked with investigators from other DIAs, and notified external agencies about the investigations where appropriate. For example, DSA investigators alerted state or federal police when there was suspected criminality in relation to a missing EO or weapon.

[126] Defence advised that DPSMS can record all relevant investigations data except for extremely large attachments (over 50 megabytes (MB)) which need to be captured and monitored in other record management systems.

4.24 For six of the 24 investigations, DPSMS records indicate that another DIA was undertaking a parallel investigation of the same security incident, and/or the relevant ADF Service unit was undertaking its own administrative inquiry of the same incident. In some of the more recent investigations, records were left open in order to monitor the outcomes of the other DIA's investigation, or the unit's administrative inquiry. However, in some of the earlier investigations from 2011 or 2012, the DSA's investigation record was closed prior to the other investigations or inquiries into the security incident being concluded.[127] More generally, as noted in Chapter 3, only a limited number of DSA staff have access to all security incidents and investigations for the purpose of high-level reporting to Defence Committees and senior management. While the DSA reports the overall number of investigations to the Defence Executive, DSA staff do not use DPSMS to otherwise monitor investigations undertaken by other DIAs.

4.25 Of the 19 closed investigations, the shortest length of time for an investigation was 11 days and the longest length of time for an investigation was 373 days. The average length of time for an investigation was 161 days. Fourteen (58 per cent) of the investigations took longer than the DSA's 90 day target period.

Outcomes of the investigations

4.26 An investigation report had been developed by the DSA for 13 of the 24 investigations. In the cases where there was not an investigation report, the reasons included: the DSA investigation had been referred to another DIA during the course of the investigation; the DSA closed its investigation on the basis that an administrative inquiry undertaken by the ADF Service unit would be a more appropriate method to address the issues leading to the EO and weapons security incident; and the DSA was unable to establish any responsible persons during the course of investigation.

4.27 The DSA investigation reports provided to the ANAO indicate some common reasons for EO and weapons security incidents. These include:

- poor controls at units or depots over EO and weapons handling;
- lack of adherence to, or poor knowledge of, extant accounting procedures for EO and weapons, in some cases resulting in EO and weapons not recorded as missing in accounting systems;

[127] These include instances where the DPSMS record for that investigation noted that the other investigation or inquiry may result in administrative action or action under the *Defence Force Discipline Act 1982*.

- security breaches including non-compliance with requirements under the DSM; and
- lack of security awareness or a disregard for some security protocols.

4.28 As previously discussed, the management of EO and weapons primarily involves the design and application of appropriate controls throughout their life cycle, from procurement, storage and handling, through to final use or disposal. However, Defence does not undertake systematic analysis of the findings of EO and weapons security investigations undertaken by the DIAs to inform its reporting to Defence senior management; a missed opportunity to establish a more robust feedback loop[128] to inform Defence EO and weapons policy and its implementation. An examination of common themes emerging from EO and weapons security investigations across the DIAs would contribute to Defence's understanding of trends and potential issues leading to EO and weapons security incidents. The findings of the reports highlight the need for Defence to reinforce, through responsible commanders and managers, the obligations that Defence personnel and contractors must meet to control and secure EO and weapons.

4.29 For the 19 closed DSA investigations, the ANAO was provided evidence that the Commanding Officer or other responsible person was provided with a written report, or other advice, detailing the outcomes of the EO and weapons security investigation. In the cases where a written report was not produced (for the reasons detailed in paragraph 4.26) there was adequate stakeholder engagement.

4.30 The DSA investigation reports included recommendations aimed at: improving the security facilities at the ADF Service unit, EO depot or warehouse; improving appropriate controls for the storage of EO; delivering training to staff responsible for the management of EO or weapons; ensuring contractor or ADF personnel comply with Defence security requirements; and improving existing procedures for accounting for EO at units or depots.

4.31 Recommendations were made as an outcome of nine of the 24 investigations conducted by the DSA. In these cases, the responsible area was requested to respond to the DSA on any actions taken to implement the recommendations within a specified timeframe, usually within three months after the completion of the investigation report. In some cases, the DPSMS

[128] As discussed in paragraph 1.4.

record for the investigation was closed prior to the deadline for the response from the relevant area in Defence.[129]

4.32 Of the nine investigations with recommendations:

- For two of the investigations, the responsible areas have advised the DSA that they have implemented the recommendations.
- For one of the investigations, the responsible areas have advised the DSA that some of the recommendations have been implemented and that the implementation of the remaining recommendations is still in progress.
- For one of the investigations, the responsible areas have advised the DSA that they will implement the recommendations.
- For four of the investigations, the DSA did not receive a response from the responsible areas on the actions that had been taken, if any, to implement the recommendations.
- For one of the investigations, the relevant area of Defence disagreed with the recommendations, and provided reasons to the DSA why it would not implement the recommendations.

4.33 In cases where the responsible area disagrees with a recommendation, the DSA can escalate the issue to ensure the recommendation is agreed to by the area. However, the DSA informed the ANAO that over the last two years, there have been no instances when it has needed to escalate an issue to ensure recommendations are implemented. During this period, the DSA also did not provide evidence of any formal action following non-responses to its requests for advice about the status of the implementation of investigation recommendations.

4.34 The outcomes of, and the recommendations from, the DSA investigations into EO and weapons security incidents highlight the importance of timely security investigations and timely implementation of investigation recommendations as an integral part of ensuring Defence's EO and weapons security. In a similar vein, the ANAO Audit Report No.25, 2012—13, *Defence's Implementation of Audit Recommendations* notes that the 'appropriate and timely implementation of recommendations that are agreed by an agency is an important part of realising the full benefits of an audit'.[130]

[129] As discussed in Chapter 3, in September 2011, the DSA's reporting team was taken offline for some 18 months to work on another major remediation project. As a result, dsaARMS was not used to monitor the implementation of recommendations from security investigation reports from September 2011 to the end of March 2013.

[130] ANAO Audit Report No.25, 2012–13, *Defence's Implementation of Audit Recommendations*, p. 5.

Conclusion

4.35 Defence has in place a range of policies, standards and procedures to guide the conduct of security investigations. These investigations are undertaken by six DIAs. There may also be multiple inquiries and investigations of a single security incident undertaken by DIAs and ADF Service units, focusing on a variety of matters including appropriate administrative action. These arrangements highlight the challenge for the DSA in monitoring EO and weapons security incident investigations and following up on their outcomes. This requires the maintenance of accurate and timely information on investigations in DPSMS.

4.36 The DSA does monitor overall numbers of EO and weapons security investigations in order to report these numbers to the Defence Executive. However, the DSA does not regularly monitor other DIAs' or ADF units' investigations and/or inquiries, nor are the outcomes routinely recorded against the DSA record for the investigation of that EO and weapons security incident. Recommendations were made as an outcome of nine of the 24 investigations conducted by the DSA. In these cases, the responsible area was requested to respond to the DSA on any actions taken to implement the recommendations within a specified timeframe, usually within three months after the completion of the investigation report. However, in some cases the responsible area did not respond to the DSA's requests for advice about implementation of recommendations. Strengthened follow-up by the DSA on the implementation of investigation recommendations, including escalation of issues with responsible senior management when appropriate, would better promote timely management action.[131]

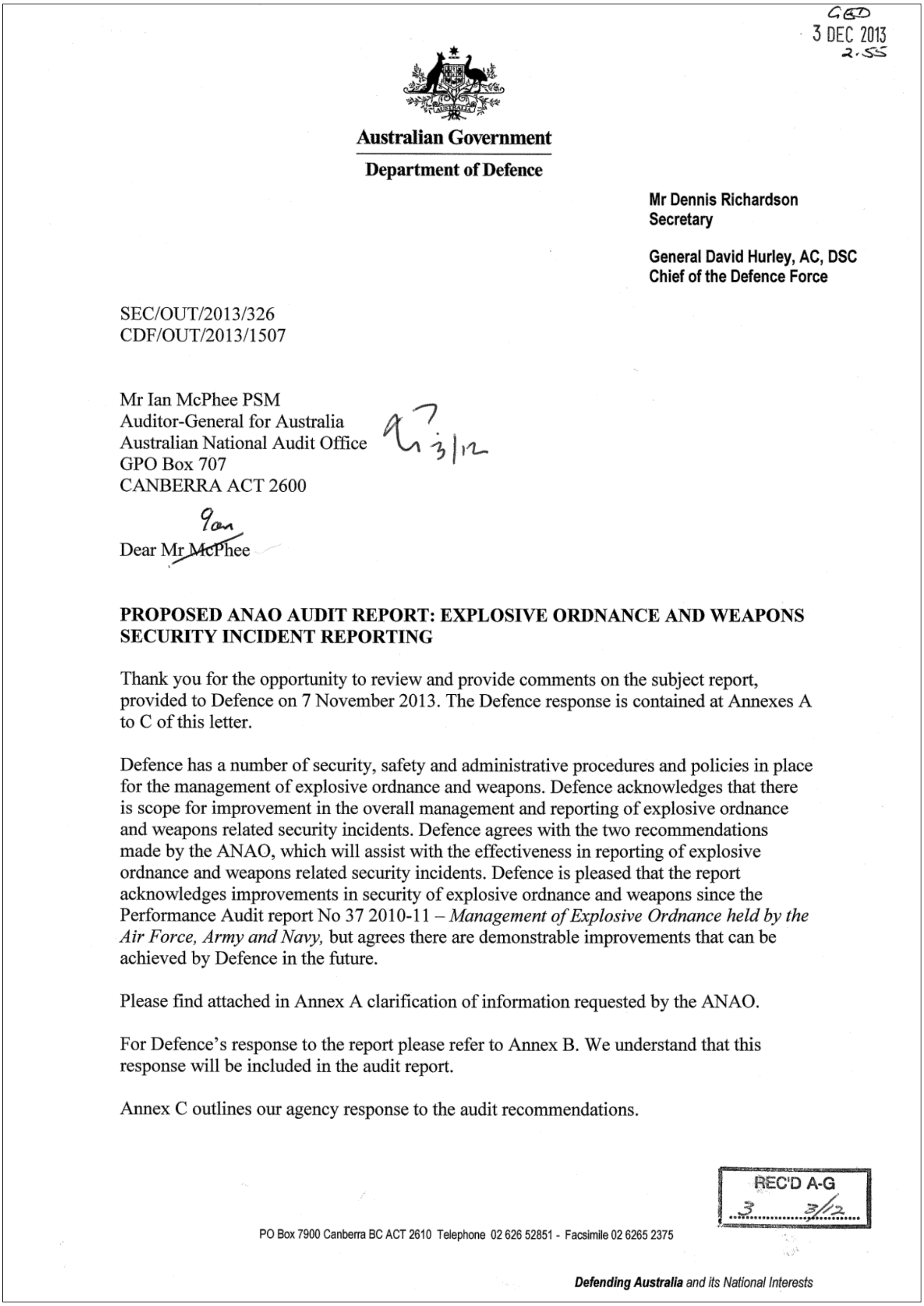
Ian McPhee
Auditor-General

Canberra ACT
18 December 2013

[131] See for example, ANAO Audit Repot No.25, 2012–13, *Defence's Implementation of Audit Recommendations* which noted that 'once agreed, audit recommendations become a management responsibility, and an effective system to implement recommendations will feature collective ownership within the agency and an action orientation which promotes timely and adequate management activity.' (p. 14).

Appendices

Appendix 1: Agency Response



Australian Government
Department of Defence

Mr Dennis Richardson
Secretary

General David Hurley, AC, DSC
Chief of the Defence Force

SEC/OUT/2013/326
CDF/OUT/2013/1507

Mr Ian McPhee PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2600

3/12

Dear Mr ~~McPhee~~ Ian

PROPOSED ANAO AUDIT REPORT: EXPLOSIVE ORDNANCE AND WEAPONS SECURITY INCIDENT REPORTING

Thank you for the opportunity to review and provide comments on the subject report, provided to Defence on 7 November 2013. The Defence response is contained at Annexes A to C of this letter.

Defence has a number of security, safety and administrative procedures and policies in place for the management of explosive ordnance and weapons. Defence acknowledges that there is scope for improvement in the overall management and reporting of explosive ordnance and weapons related security incidents. Defence agrees with the two recommendations made by the ANAO, which will assist with the effectiveness in reporting of explosive ordnance and weapons related security incidents. Defence is pleased that the report acknowledges improvements in security of explosive ordnance and weapons since the Performance Audit report No 37 2010-11 – *Management of Explosive Ordnance held by the Air Force, Army and Navy,* but agrees there are demonstrable improvements that can be achieved by Defence in the future.

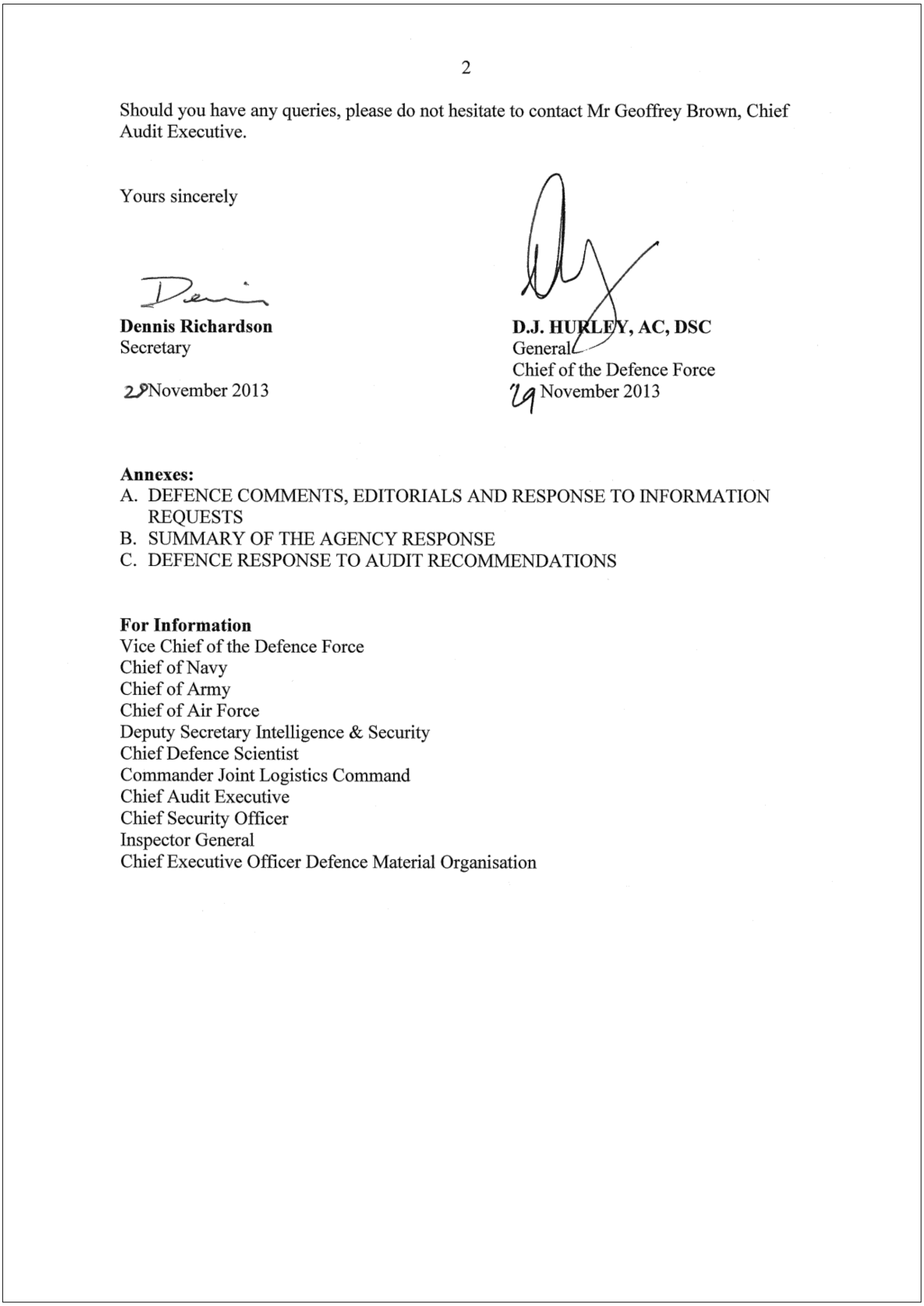
Please find attached in Annex A clarification of information requested by the ANAO.

For Defence's response to the report please refer to Annex B. We understand that this response will be included in the audit report.

Annex C outlines our agency response to the audit recommendations.

PO Box 7900 Canberra BC ACT 2610 Telephone 02 626 52851 - Facsimile 02 6265 2375

Defending Australia *and its National Interests*



2

Should you have any queries, please do not hesitate to contact Mr Geoffrey Brown, Chief Audit Executive.

Yours sincerely

Dennis Richardson
Secretary

29November 2013

D.J. HURLEY, AC, DSC
General
Chief of the Defence Force
29 November 2013

Annexes:

A. DEFENCE COMMENTS, EDITORIALS AND RESPONSE TO INFORMATION REQUESTS
B. SUMMARY OF THE AGENCY RESPONSE
C. DEFENCE RESPONSE TO AUDIT RECOMMENDATIONS

For Information
Vice Chief of the Defence Force
Chief of Navy
Chief of Army
Chief of Air Force
Deputy Secretary Intelligence & Security
Chief Defence Scientist
Commander Joint Logistics Command
Chief Audit Executive
Chief Security Officer
Inspector General
Chief Executive Officer Defence Material Organisation

Appendix 2: Defence's Definitions of EO and Weapons

Explosive Ordnance

Explosive ordnance is defined as all munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. This includes:

- bombs and warheads;
- guided and ballistic missiles;
- artillery, mortar, rocket and small arms ammunition;
- all mines, torpedoes and depth charges;
- demolition charges;
- pyrotechnics;
- clusters and dispensers;
- cartridge and propellant actuated devices;
- electro-explosive devices;
- clandestine and other improvised explosive devices; and
- all similar or related items or components explosive in nature.

Defence Explosive Ordnance Publication 101 (DEOP 101), contains a similar definition of EO and adds to the definition, in the context of EO incident reporting, all similar and related EO components that are non-explosive (inert) in nature (including containers and packaging). DEOP 101 is the primary source of regulations, principles, standards and procedures for the management and safety of EO in Defence.

Weapon

The term 'weapon' in the context of Defence security requirements includes both a 'Defence weapon' and a 'cadet firearm'. A 'Defence weapon' is defined as a weapon owned by Defence to meet the operational, training and support requirements of the Permanent and Reserve members of the Australian Defence Force (ADF). For the purposes of differentiating storage and transportation security requirements, Defence groups Defence weapons into subcategories including:

- small arms (less than 20 mm calibre; and greater than 20 mm calibre and able to be carried by one person);
- large weapons (20 mm calibre or greater and not able to be carried by one person);
- controlled repair parts (components and sub-assemblies that require the same security measures as a complete weapon);
- edged weapons (for example, combat knives and bayonets);
- innocuous weapons (which have been rendered incapable of discharging a projectile); and
- replica Defence weapons (inert items made to replicate the size and weight of a live firing Defence weapon, or its component parts, for the purpose of training).

'Cadet firearms' are not Defence weapons but are approved by Defence for use by cadets. Cadet firearms are generally weapons that are commercially available to the public, subject to state and territory laws and regulations.

Source: Department of Defence, Defence Security Manual, Part 2:67, Version 5, September 2012, p. 2 and Part 2:66, Version 6, September 2012, pp. 2–3; Defence Explosive Ordnance Publication 101 (DEOP 101), Regulation 1.3 Explosive Ordnance Incidents, p. 1.

Appendix 3: Significant Stakeholders in the Management of EO and Weapons Security Incidents in Defence

Element of Defence	Roles and Responsibilities
Chief Security Officer (CSO)	• The Chief of the Defence Force (CDF) and the Secretary of Defence have designated the CSO as the Agency Security Adviser (ASA) for Defence. In this role, the CSO must perform all of the responsibilities mandated of an ASA and, as such, is responsible for ensuring that Defence's policies and practices within the DSM remain valid and current with Australian Government requirements, as published from time to time, and meet Defence's business needs. • The CSO and the Service Security Authorities (SSA) are responsible for the provision of advice regarding security incident reporting and security investigations (The SSAs perform this function for their respective Services). • Ensures that reported security incidents have been recorded in the Defence Policing and Security Management System (DPSMS).[132] • Analyses all reported security incidents. • Determines the security incidents which need to be investigated. • Determines the most appropriate Defence Investigative Authority, Civil Authority or unit to conduct an investigation or administrative inquiry in the event of a major security incident. • At the completion of an investigation into a security incident, the Defence Investigative Authority must provide the CSO with an investigation report detailing actions undertaken throughout the course of the investigation, the findings of the investigation and any remedial recommendations. The CSO is required to ensure that recommendations from the investigation are assigned for implementation to all areas of Defence affected by the recommendations. • Consults with the Australian Security Intelligence Organisation (ASIO) and other law enforcement agencies prior to commencing an investigation to determine which agency will take responsibility for investigating a reportable major security incident.

[132] DPSMS is the primary and approved corporate computerised system for recording all reports of, and investigations into, major security incidents within Defence. Source: Defence Security Manual, Part 2:12, Security Incidents and Investigations, Version 4, September 2012, p. 9.

Element of Defence	Roles and Responsibilities
Defence Security Authority (DSA) – includes the Defence Security Incident Centre and the Security Investigation Unit.	• Set Defence protective security policy including Defence's primary source of protective security policy, the Defence Security Manual. • Be the Defence point of contact on protective security matters. • Assist the Secretary, Chief of the Defence Force, Group Heads and Service Chiefs to manage security risks and implement security policy. • Monitor and report on security compliance, performance and risks including the management of the Defence Security Authority Audit Recommendation Management System (dsaARMS), which includes security compliance, performance and investigation report recommendations and consolidates these into a single, national database. • The Security Incident Centre assesses, refers and analyses security incidents in Defence. • The Security Investigations Unit investigates major security incidents that may be in breach of the DSM and its referenced authoritative texts, or any relevant legislation as directed by the CSO; and examines serious and complex security incidents that may significantly damage Defence capability or its reputation, such as incidents concerning weapons, munitions and explosives. • Security clearance vetting for the whole-of-government; under the auspices of the Australian Government Security Vetting Agency (AGSVA).
Defence Investigative Authority (DIA)	The DIA bodies are the: – Australian Defence Force Investigative Service (ADFIS); – Service police organisations of the Army, Navy and Air Force; – the Directorate of Security Intelligence and Investigations within the Defence Security Authority (DSA); and – Directorate of Investigation and Recovery within the Inspector General Division. The six DIA bodies within Defence are authorised by the Secretary and CDF to conduct formal investigations. It is their responsibility to: • Conduct investigations in accordance with the Defence and the Australian Government Investigating Standards. • Log security incidents reported to the Defence investigative authority onto the DPSMS. • Report all major security incidents to the Security

Element of Defence	Roles and Responsibilities
	Incident Centre through the DPSMS. • Inform the Executive Director Vetting where an investigation makes an adverse finding against an individual, including where the event was accidental. Results and circumstances must be recorded on the individual's Personal Security File. • At the completion of an investigation into a security incident, the DIA must provide the CSO with an investigation report detailing actions undertaken throughout the course of the investigation, the findings of the investigation and any remedial recommendations.
Defence Group Heads	• Group Heads must assign an officer at or above the SES Band 1 to be responsible for implementing the recommendations from a security investigation. The appointed officer must report back to the CSO on action taken in response to the recommendation within three months of the investigation report, or other timeframe specified by the CSO.
ADF Service (Air Force, Army, Navy) Chiefs	• Ensure the security of EO and weapons under their control. • Service Chiefs must assign an officer at or above 'O7 level' (being ADF 'one-star' ranks of Air Commodore (Air Force), Brigadier (Army) or Commodore (Navy)) to be responsible for implementing the recommendations from a security investigation. The appointed officer must report back to the CSO on action taken in response to the recommendation within three months of the investigation report, or other timeframe specified by the CSO.
Service Security Authorities (SSA)	Provide advice regarding security incident reporting and security investigations for their respective ADF Service.
Commanders and managers	• Ensure that they and their staff are aware of, and comply with, the requirement to report and manage all security incidents. • Ensure the security of EO and weapons under their control, including when on issue to their staff, and ensure compliance with the requirements of the DSM. They must, among other things: – secure and account for all EO and weapons on charge to, or in the custody of, units under their control; and – review any EO and weapons related unit security instructions.

Element of Defence	Roles and Responsibilities
Security Officers	• Report all security incidents and record them in the security register. • Ensure that all major security incidents are reported to the Security Incident Centre, which will determine the incidents to be investigated by a DIA and determine the appropriate DIA for such investigation. • Assist commanders and managers to educate staff on their security responsibilities in relation to security incidents and investigation. • Assist Defence personnel and external service providers to complete the reporting requirements for security incidents and investigations in accordance with the instructions given in the DSM.
Director General, Explosive Ordnance – Joint Logistics Command.	The Director General Explosive Ordnance (DGEO) is responsible for leading the management of EO in Defence including the governance of the Weapons, Munitions and Explosives Program within JLC. DGEO reports to and supports Commander Joint Logistics (CJLOG) as the single point of accountability for ensuring the overall system performance of defence logistics. CJLOG, in turn, supports the Vice Chief of the Defence Force (VCDF) as the single point of accountability for explosive ordnance and weapons in Defence, a responsibility given to VCDF in response to Recommendation 1 of the 2007 Security Performance Audit of Weapons Munitions and Explosives.

Source: ANAO analysis of Defence documentation.

Note: The Security Performance Audit of Weapons Munitions and Explosives (2007 WME Audit) recommended that VCDF, assisted by CJLOG, provide oversight, coordination and assurance of the efficiency and effectiveness of the overall WME system. Defence subsequently established VCDF as the single point of accountability for matters relating to EO with responsibility for the oversight, coordination and assurance of the efficiency and effectiveness of the overall explosive ordnance system. The 2007 WME Audit is discussed further in paragraph 1.16.

Appendix 4: Case Studies of EO and Weapons Security Incidents

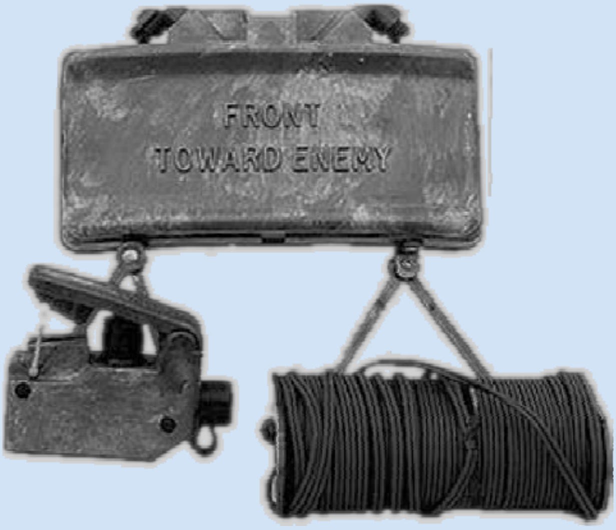
Lack of adherence to EO handling procedures

Loss of Claymore Antipersonnel Weapon – Queensland – January 2011

Incident date: Lost between 25 and 28 January 2011.

Reported to DSA: 4 February 2011.

Description of item: The antipersonnel Weapon M18A1 Claymore (Claymore) is a weapon designed primarily for use against personnel. The fragments can also penetrate unarmoured vehicles. The Claymore contains 680 grams of explosive and, when detonated, fires approximately 700 steel balls of 3.2mm diameter at a velocity of 4 320km/h out to about 100m within a 60° arc in front of the device (the danger area consists of a 180° arc out to approximately 250m). A picture of a Claymore is shown below.



Description of the incident: Between 15 and 28 January 2011, the Army conducted a training course for reservists at the Greenbank Training Area, Greenbank, Queensland. A number of Claymores were delivered to the training area as part of the explosive ordnance supplies required for the training course.

On 28 January 2011, at the end of the training course, unused explosive ordnance was collected by Defence's civilian contractor for explosive ordnance services and returned to its depot where it was discovered that one Claymore was missing from the items collected.

Army personnel conducted searches of a landfill area as it was thought that the Claymore may have been accidentally disposed of in an industrial skip bin with the packaging from other explosive ordnance from the training activity. The skip bin was collected by civilian contractors on 1 February 2011 with the contents eventually dumped in landfill. The Claymore was not found.

The ADFIS investigations into the incident found that the Army personnel involved in the training exercise did not comply with Defence's regulations for accounting for explosive ordnance and this directly resulted in the loss of the Claymore and the loss not being discovered until 11 days later.

An inquiry into the incident by Army identified a number of systemic issues associated with non compliance with mandated ADF policy. Additionally, an Army review of its range practice activities identified systemic weaknesses and inconsistencies in Army's culture, record-keeping, service specific and unit level instructions, risk management practices and personnel management.

Defence has been unable to determine the whereabouts of the Claymore.

No action has been taken against any Defence personnel for the non-compliance with Defence procedures despite the ADFIS investigation recommending that action be taken against one of the individuals involved in the incident.

Source: ANAO analysis of Defence documentation and the following media articles: http://www.theaustralian.com.au/national-affairs/policy/justice-delayed-by-cops-as-mps-confined-to-base/story-e6frg8yo-1226422941601#mm-premium; http://www.theage.com.au/national/army-reservists-search-in-rubbish-dump-for-lost-mine-20110325-1ca63.html; and http://www.smh.com.au/national/fruitless-army-mine-search-cost-500000-20110325-1ca76.html. [Accessed 28 November 2013].

ADF unit incorrect assessment of an EO incident as not being a security incident

Various EO found in ADF member's former residence

Incident date: 19 April 2013

Reported to DSA: 1 May 2013

Description of incident

Defence was advised by Queensland Police of explosive ordnance and other items including grenades and trip wires, reportedly belonging to an ADF member, in a Queensland residence. ADF EO disposal specialists were called in by the police to assist with identification and removal of the items found. The incident had been reported to police by a member of the public. The ADF EO staff did not report the incident to the DSA as a security incident via an XP-188 form as is required by Defence policy even though it had potential security implications. The police advised Defence that the ADF member concerned had been charged with stealing and possession of a 'Category R' weapon.[133] When the DSA did become aware of the incident, further enquires by the DSA revealed 162 other EO incidents that had not been reported as security incidents to the DSA.

Source: ANAO analysis of Defence documentation.

[133] Under Queensland law, the definition of a Category R weapon includes but is not limited to machine guns and fully automatic large calibre military weapons. Examples include any fully automatic gun (including replicas); hand grenade; antipersonnel mine; rocket launcher, recoilless rifle, antitank rifle; a rocket propelled grenade type launcher; a mortar; and all artillery. These weapons are effectively banned in Australia outside of strictly controlled requirements for use in military, police, other government or special circumstances.

Other examples of EO and weapons security incidents

Other examples of investigations into EO and weapons security incidents

- Weapons stolen from Defence in 2001 are discovered in the hands of a known criminal in 2010 when handed to police as part of a deal to reduce his sentence.
- Cultural issues in the ADF contributing to situations where Defence policies and procedures are not followed resulting in live EO being treated as inert (2011).
- Grenade recovered by police as part of gang dispute (2012).
- Incorrect handling and stocktaking procedures for weapons and EO contribute to items being unaccounted for (2011 and 2013).
- Ammunition found in public areas that Defence did not know it had lost (2011 and 2012).
- EO found in homes of former ADF personnel (2011 and 2012).
- Items declared destroyed reappear at a later date (2010).
- Plastic explosives missing from delivery (2012).
- Plastic and sheet explosives discovered missing from Defence range and not recovered (2013).
- Plastic explosives missing from unit stores (2013). On 29 August 2013, Defence advised the ANAO that this investigation was ongoing.
- Weapons and EO left unsecure in breach of Defence requirements (2011, 2012).

Source: ANAO analysis of Defence documentation.

Appendix 5: ANAO Survey

41. The ANAO survey was completed online and included multiple choice questions, questions with rating scales, and free text questions. The survey was open to respondents from 3 May 2013 to 31 May 2013.

42. The survey included 49 respondents based at the following Defence establishments across Australia[134]:

- Royal Military College, Duntroon, ACT;
- HMAS Albatross, Nowra, NSW;
- HMAS Waterhen, Waverton, NSW;
- Blamey Barracks, Kapooka, NSW;
- Lone Pine Barracks, Singleton, NSW;
- Randwick Barracks, Randwick, NSW;
- RAAF Base Darwin, Winnellie, NT;
- RAAF Base Tindal, Tindal, NT;
- Gallipoli Barracks, Enoggera, QLD;
- RAAF Base Amberley, Amberley, QLD;
- RAAF Base Townsville, Townsville City, QLD;
- RAAF Base Edinburgh / Edinburgh Defence Precinct, Edinburgh, SA;
- RAAF Base East Sale, East Sale, VIC;
- RAAF Other bases;
- HMAS Stirling, Garden Island, WA; and
- EO Depots (Orchard Hills, Myambat, Jennings, NSW and Townsville, QLD).

43. The table below indicates the Service or area of Defence in which the survey respondents work.

[134] One survey respondent did not specify the Defence establishment at which they were located.

Survey respondents’ Service or area of Defence

Service or Area of Defence	Number of Survey Respondents
Army	6[135]
Navy	4
Air Force	28
Contractor	9
Other[136]	2
Total	**49**

Source: Survey results.

[135] The low number of Army responses is due to a large number of Army personnel being on training exercises during the period in which the survey was open for response.

[136] Two of the survey respondents did not specify the Service or area of Defence in which they worked.

Survey Results

A. Explosive ordnance / weapons security incidents	
How many explosive ordnance (EO) or weapons security incidents have occurred in your unit or depot over the last 12 months?	
	Per cent
None	57
1-5	34
5-10	2
> 10	7
Were these incidents the result of: (multiple response)	
	Per cent
an accounting error	35
a loss	26
a theft	-
a found item (for example, World War II munitions)	34
a Free From explosives (FFE) incident	22
Other[137]	30
Not sure	17
Have you directly been involved in any EO and weapons incidents, or reported any incidents, in the past 12 months	
	Per cent
Yes	52
No	48
For any EO and weapons incidents that you have reported or been involved in, were you informed of the outcome of any resulting investigation?	
	Per cent
Yes	73
No	27
Are you aware of any EO or weapons incidents that have not been reported in accordance with Defence policies and procedures?	
	Per cent
Yes[138]	17
No	83

[137] Reasons provided mostly relate to procedures not being followed.

[138] Reasons for not reporting in accordance with Defence procedures were: not worth reporting; procedures not followed due to higher level management downplaying the seriousness of the issue; the incident was the result of an accounting error.

B. Guidance for reporting security incidents	
What resources or documents do you use as guidance in reporting EO or weapons security incidents (multiple response)	
	Per cent
The electronic Defence Security Manual (eDSM)	98
Defence Instructions General (DIGs)	46
Service-specific Instructions	46
The Defence Intranet on the Defence Restricted Network (DRN)	46
The electronic Defence Explosive Ordnance Publication 101 (eDEOP 101) – Department of Defence Explosives Regulations – Regulation 1.3	81
Sought advice directly from:	
- the Defence Security Authority (DSA) (via phone call or email)	35
- another Defence Investigative Authority (DIA) (via phone call or email)	4
- the base security area (via phone call or email)	19
- the relevant Joint Logistics Unit (JLU) – Regional EO Services Office	44
- the EO Incident Administration Cell (EOIAC)	6
Other	10
Please rate your satisfaction with the usefulness of the guidance available to you in reporting EO or weapons security incidents	
	Per cent
The electronic Defence Security Manual (eDSM)	
Very satisfied	17
Satisfied	59
Neither satisfied nor dissatisfied	17
Dissatisfied	4
Very dissatisfied	2
Defence Instructions General (DIGs)	**Per cent**
Very satisfied	3
Satisfied	50
Neither satisfied nor dissatisfied	39
Dissatisfied	6
Very dissatisfied	3

B. Guidance for reporting security incidents (continued)	
Service-specific Instructions	**Per cent**
Very satisfied	-
Satisfied	60
Neither satisfied nor dissatisfied	31
Dissatisfied	3
Very dissatisfied	6
The Defence Intranet on the Defence Restricted Network (DRN)	**Per cent**
Very satisfied	3
Satisfied	60
Neither satisfied nor dissatisfied	27
Dissatisfied	11
Very dissatisfied	-
The electronic Defence Explosive Ordnance Publication 101 (eDEOP 101) – Department of Defence Explosives Regulations – Regulation 1.3	**Per cent**
Very satisfied	9
Satisfied	66
Neither satisfied nor dissatisfied	23
Dissatisfied	2
Very dissatisfied	-
Advice directly from the Defence Security Authority (DSA) (via phone call or email)	**Per cent**
Very satisfied	13
Satisfied	40
Neither satisfied nor dissatisfied	37
Dissatisfied	10
Very dissatisfied	-
Advice directly from another Defence Investigative Authority (DIA) (via phone call or email)	**Per cent**
Very satisfied	5
Satisfied	25
Neither satisfied nor dissatisfied	65
Dissatisfied	-
Very dissatisfied	5

B. Guidance for reporting security incidents (continued)	
Advice directly from the base security area (via phone call or email)	**Per cent**
Very satisfied	4
Satisfied	42
Neither satisfied nor dissatisfied	50
Dissatisfied	4
Very dissatisfied	-
Advice directly from the relevant Joint Logistics Unit (JLU) – Regional EO Services Office	**Per cent**
Very satisfied	7
Satisfied	63
Neither satisfied nor dissatisfied	27
Dissatisfied	-
Very dissatisfied	3
Advice directly from the EO Incident Administration Cell (EOIAC)	**Per cent**
Very satisfied	10
Satisfied	15
Neither satisfied nor dissatisfied	65
Dissatisfied	5
Very dissatisfied	5
Are you aware of any changes to policies and procedures for reporting EO and weapons security incidents at your unit or depot over the past 12 months as a result of an EO or weapons security incident?	
	Per cent
Yes	29
No	71
How would you rate the overall impact these changes have had on your unit's or depot's ability to report and investigate EO or weapons security incidents?	
	Per cent
Large positive effect	18
Small positive effect	36
No effect	36
Small negative effect	9
Large negative effect	-

B. Guidance for reporting security incidents (continued)

Have you received any training on procedures and policies for reporting EO and weapons security incidents?

	Per cent
Yes	59
No	41

How was this training conducted? (multiple responses)

	Per cent
On the job	78
Reading manuals, policies and procedures	82
Training from an external provider	30
Other	11

C. Reporting security incidents

What forms / reporting lines have you used in the past 12 months to report an EO or weapons security incident? (multiple response)

	Per cent
An XP188 form	41
An EO incident form (EO016)	57
Verbal or written report to Unit Commander or Management	33
Verbal or written report to Unit Security Officer	24
Verbal or written report to Base Security Officer	10
Verbal or written report to Defence Security Authority (DSA)	10
Verbal or written report to the relevant Joint Logistics Unit (JLU) Regional EO Services	19
Verbal or written report to the EO Incident Administration Cell (EOIAC)	2
Other	29

How would you rate the usability of the XP188 form?

	Per cent
Very easy to use	19
Easy to use	31
Neither easy nor difficult to use	44
Difficult to use	6
Very difficult to use	-

C. Reporting security incidents (continued)

Does your unit/depot/Service maintain specific log of EO or weapons security incidents? (multiple response)

	Per cent
Yes, my unit maintains a log	44
Yes, my depot maintains a log	17
Yes, my Service maintains a log	6
No	6
Not sure	29

What formats are the security incident logs stored in? (multiple response)

	Per cent
Hardcopy	58
Electronic format	87
Not sure	7

What general types of information is kept in this log? (multiple response)

	Per cent
Date of incident	100
Location of incident	97
Type of incident	100
Weapon or EO type/description	90
Reporting officer(s)	90
Outcomes	69

D. Overall satisfaction with guidance and processes for reporting security incidents

Please indicate your level of agreement with the following statements in relation to EO and weapons security incidents in Defence.

I know where I can find policy and procedures about reporting an EO or weapons security incident.

	Per cent
Strongly agree	23
Agree	65
Neither agree nor disagree	10
Disagree	2
Strongly disagree	-

D. Overall satisfaction with guidance and processes for reporting security incidents (continued)	
I understand how EO and weapons security policies and procedures relate to the work I do.	
	Per cent
Strongly agree	30
Agree	62
Neither agree nor disagree	9
Disagree	-
Strongly disagree	-
I know how to report an EO or weapons security incident.	
	Per cent
Strongly agree	26
Agree	60
Neither agree nor disagree	15
Disagree	-
Strongly disagree	-
I know who to report the incident (EO or weapons security) to.	
	Per cent
Strongly agree	30
Agree	60
Neither agree nor disagree	11
Disagree	-
Strongly disagree	-
Command and Management take all EO and weapons security incidents seriously.	
	Per cent
Strongly agree	46
Agree	35
Neither agree nor disagree	15
Disagree	2
Strongly disagree	2

D. Overall satisfaction with guidance and processes for reporting security incidents (continued)	
Command and Management support staff in reporting EO and weapons security incidents.	
	Per cent
Strongly agree	40
Agree	40
Neither agree nor disagree	17
Disagree	2
Strongly disagree	2
Command and Management take appropriate action in relation to all EO and weapons security incidents.	
	Per cent
Strongly agree	40
Agree	40
Neither agree nor disagree	15
Disagree	2
Strongly disagree	4
The processes for reporting EO and weapons security incidents have been communicated effectively across the ADF and the Department.	
	Per cent
Strongly agree	4
Agree	40
Neither agree nor disagree	36
Disagree	19
Strongly disagree	-
There is a consistent approach to reporting and investigating EO and weapons security incidents across Defence.	
	Per cent
Strongly agree	7
Agree	39
Neither agree nor disagree	41
Disagree	7
Strongly disagree	7

D. Overall satisfaction with guidance and processes for reporting security incidents (continued)	
Assessing, recording and reporting EO and weapons security incidents are important aspects of maintaining security at units and depots.	
	Per cent
Strongly agree	48
Agree	44
Neither agree nor disagree	8
Disagree	-
Strongly disagree	-
Defence processes on reporting EO and weapons security incidents are detailed and specific.	
	Per cent
Strongly agree	11
Agree	68
Neither agree nor disagree	15
Disagree	4
Strongly disagree	2
Defence processes on reporting EO and weapons security incidents are clear.	
	Per cent
Strongly agree	11
Agree	62
Neither agree nor disagree	21
Disagree	4
Strongly disagree	2
Please rate your overall satisfaction with the guidance and processes for reporting security incidents.	
	Per cent
Very satisfied	10
Satisfied	58
Neither satisfied nor dissatisfied	29
Dissatisfied	-
Very dissatisfied	2

Source: ANAO May 2013 survey of Defence staff.

Note: Percentages do not add to 100 per cent due to rounding.

Index

Series Titles

ANAO Audit Report No.1 2013–14
Design and Implementation of the Liveable Cities Program
Department of Infrastructure and Transport

ANAO Audit Report No.2 2013–14
Administration of the Agreements for the Management, Operation and Funding of the Mersey Community Hospital
Department of Health and Ageing
Department of Health and Human Services, Tasmania
Tasmanian Health Organisation – North West

ANAO Audit Report No.3 2013–14
AIR 8000 Phase 2 — C-27J Spartan Battlefield Airlift Aircraft
Department of Defence

ANAO Audit Report No.4 2013–14
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2012 Compliance)
Across Agencies

ANAO Audit Report No.5 2013–14
Administration of the Taxation of Personal Services Income
Australian Taxation Office

ANAO Audit Report No.6 2013–14
Capability Development Reform
Department of Defence

ANAO Audit Report No.7 2013–14
Agency Management of Arrangements to Meet Australia's International Obligations
Across Agencies

ANAO Audit Report No.8 2013–14
The Australian Government Reconstruction Inspectorate's Conduct of Value for Money Reviews of Flood Reconstruction Projects in Queensland
Department of Infrastructure and Regional Development

ANAO Audit Report No.9 2013–14
Determination and Collection of Financial Industry Levies
Australian Prudential Regulation Authority
Department of the Treasury

ANAO Audit Report No.10 2013–14
Torres Strait Regional Authority — Service Delivery
Torres Strait Regional Authority

ANAO Audit Report No.11 2013–14
Delivery of the Filling the Research Gap under the Carbon Farming Futures Program
Department of Agriculture

ANAO Report No.12 2013-14
2012–13 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.13 2013-14
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2013
Across Agencies

ANAO Audit Report No.14 2013-14
Explosive Ordnance and Weapons Security Incident Reporting
Department of Defence

Current Better Practice Guides

The following Better Practice Guides are available on the ANAO website.

Implementing Better Practice Grants Administration	Dec. 2013
Preparation of Financial Statements by Public Sector Entities	June 2013
Human Resource Management Information Systems – Risks and Controls	June 2013
Public Sector Internal Audit	Sept. 2012
Public Sector Environmental Management	Apr. 2012
Developing and Managing Contracts – Getting the right outcome, achieving value for money	Feb. 2012
Public Sector Audit Committees	Aug. 2011
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities – Delivering agreed outcomes through an efficient and optimal asset base	Sept. 2010
Planning and Approving Projects – an Executive Perspective	June 2010
Innovation in the Public Sector – Enabling Better Performance, Driving New Directions	Dec. 2009
SAP ECC 6.0 – Security and Control	June 2009
Business Continuity Management – Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Fairness and Transparency in Purchasing Decisions – Probity in Australian Government Procurement	Aug. 2007
Administering Regulation	Mar. 2007
Implementation of Program and Policy Initiatives – Making implementation matter	Oct. 2006