The Auditor-General
Audit Report No.37 2010–11
Performance Audit

Management of Explosive Ordnance Held by the Air Force, Army and Navy

Department of Defence

Australian National Audit Office

© Commonwealth
of Australia 2011

ISSN 1036–7632

ISBN 0 642 81183 0

COPYRIGHT INFORMATION

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to:

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

Or via email:
webmaster@anao.gov.au

Australian National
Audit Office

Canberra ACT
19 April 2011

Dear Mr President
Dear Mr 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 and the accompanying brochure to the Parliament. The report is titled *Management of Explosive Ordnance Held by the Air Force, Army and Navy.*

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—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 and financial statement audits 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

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team
Natalie Whiteley
Kim Murray
Michael Kozakos
Kim Bond

Contents

Abbreviations 7

Summary and Recommendations 9

Summary 11
Introduction 11
Audit approach 15
Overall conclusion 15
Key Findings 18
Summary of agency response 24
Recommendations 25

Audit Findings 27

1. Introduction 29
Background 29
Defence's explosive ordnance inventory 34
Reviews and reforms of the explosive ordnance domain within Defence 38
Single point of accountability for explosive ordnance in Defence 43
Systems used to account for explosive ordnance inventory in Defence 43
Audit approach 44
Report structure 47
2. Reviews and Reforms of Explosive Ordnance Management 48
Introduction 48
Ongoing monitoring and review at the unit level 52
Recommendation No.1 55
Reform of the explosive ordnance management functions within Defence 55
3. Management of Explosive Ordnance at ADF Units 58
Framework for the management of explosive ordnance at units 58
Recommendation No.2 66
Requirements for units to account for explosive ordnance 66
Training in explosive ordnance accounting available to unit personnel 73
4. Information and Records Management Systems 74
Introduction 74
Overview of explosive ordnance inventory management systems in Defence 77
Computer System for Armaments 80
Standard Defence Supply System 84
Stocktaking of explosive ordnance at units 87
Inventory Management Systems used by the Services 92
Recommendation No.3 96

5. Security and Security Incident Management for Explosive Ordnance at Units 97
Introduction 97
Defence's requirements for managing explosive ordnance security incidents 98
Recommendation No.4 106
Defence ban on unaccompanied access to explosive ordnance 106
Management of explosive ordnance security incidents 108
Recommendation No.5 115
Appendices 117
Index 119
Series Titles 120
Current Better Practice Guides 124

Tables

Table 1.1 Significant stakeholders in the aspects of explosive ordnance management in Defence discussed in this audit 33
Table 1.2 Defence's explosive ordnance inventory balances as at 30 June in the last three financial years 35
Table 1.3 Significant reviews and reforms in Defence's explosive ordnance domain 39
Table 1.4 ADF units and bases visited as part of audit fieldwork 46
Table 2.1 2007 WME Audit findings and recommendations relating to management of explosive ordnance at the unit level 50
Table 2.2 Explosive Ordnance Reform Program 56
Table 3.1 Key Defence Instructions (General) relating to the physical control of explosive ordnance at units 62
Table 3.2 Other key Defence requirements relating to the physical control of explosive ordnance at units 64
Table 4.1 Explosive ordnance inventory management systems in Defence 77
Table 4.2 Units identified in COMSARM as 'auto-consuming' or 'non auto-consuming' 82
Table 4.3 Instructions and procedures for stocktaking explosive ordnance by ADF Service 89
Table 5.1 Requirements for reporting of explosive ordnance related security incidents 105
Table 5.2 Reported security incidents involving the loss of explosive ordnance from 2008 to 10 May 2010 110

Figures

Figure 1.1 Key stages in the management of explosive ordnance in Defence 30
Figure 1.2 Management of explosive ordnance at the unit level in Defence 31
Figure 3.1 Defence's System of Defence Instructions 60
Figure 4.1 Key information management systems used by the Services to account for explosive ordnance (excluding operations) 79

Abbreviations

ADF	Australian Defence Force
ANAO	Australian National Audit Office
CDF	Chief of the Defence Force
CJLOG	Chief of the Joint Logistics Command
COMSARM	Computer System for Armaments
DEOC	Defence Explosive Ordnance Committee
DEOP	Defence Explosive Ordnance Publication
DEOS	Directorate of Explosive Ordnance Services
DEOTS	Defence Explosive Ordnance Training School
DI(G)	Defence Instruction (General)
DMO	Defence Materiel Organisation
DPSMS	Defence Policing and Security Management System
DSA	Defence Security Authority
DSG	Defence Support Group
DSPR	Directorate of Security Performance Review
ECOMS	Explosives Custodian Officer Management System
DSM	Defence Security Manual
EOMA	Explosive Ordnance Monitoring Authority
EOS	Explosive Ordnance Services
ESCM	Electronic Supply Chain Manual

GSS	Garrison Support Services
JLC	Joint Logistics Command
M72	M72A76 – Light Anti-Armour Weapon
MILIS	Military Integrated Logistics Information System
PSM	Australian Government Protective Security Manual
RAAF	Royal Australian Air Force
RAN	Royal Australian Navy
ROMAN	Resource Output Management and Accounting Network
SDSS	Standard Defence Supply System
SoDI	Systems of Defence Instructions
SRS	Stocktake Reporting System
UDC	Unit Designator Code
VCDF	Vice Chief of the Defence Force
WME	Weapons, Munitions and Explosives

Summary and Recommendations

Summary

Introduction

1. The effective management of explosive ordnance[1] is integral to military capability and is essential to military operations. Explosive ordnance management is a core function of the Australian Defence Force (ADF) and involves considerable levels of expenditure. At 30 June 2010, the Department of Defence (Defence) reported explosive ordnance inventory of $3.1 billion,[2] (some 60 per cent of Defence's reported total inventory at that date) comprising mainly the inventory of the 17 depots managed by Joint Logistics Command (JLC), from which explosive ordnance is issued to ADF units.

2. The main focus of this audit is Defence's management of explosive ordnance inventory after it has left the depots and has become the responsibility of Air Force, Navy and Army units. It is at this point that Defence's explosive ordnance is most widely dispersed and at greatest risk of loss or theft. The *Defence Security Manual* (DSM)[3] imposes correspondingly important responsibilities on ADF unit commanders and managers, including the responsibility to:

> secure and account for all [*explosive ordnance*] on charge to, or in the custody of, units under their control.[4]

3. The critical nature of these responsibilities has been highlighted by a number of high-profile safety and security incidents involving explosive

---

1 Explosive ordnance consists of 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. Source: Department of Defence, *Defence Security Manual*, 2009.

2 Defence's inventory is reported at cost, adjusted where applicable for loss of service potential. The costs of inventories are assigned by using a weighted average cost formula. Department of Defence, *Defence Annual Report 2009–10*, Volume 1, p. 214. The total explosive ordnance inventory reported in financial statements is based on the information held in Defence's Computer System for Armaments (COMSARM), plus adjustments for some transactions not recorded in COMSARM. Explosive ordnance inventory recorded in other systems used by ADF units is not reflected in the total explosive ordnance inventory reported in Defence's financial statements.

3 Department of Defence, *Defence Security Manual*, 2009 was the current version of this manual at the time of fieldwork for this audit.

4 Department of Defence, *Defence Security Manual*, 2009, paragraph 67.22 (a).

ordnance that have been the subject of internal and external scrutiny over recent years. In late December 2006, the then Minister for Defence announced an internal security performance audit of Defence's weapons, munitions and explosives.[5] This followed advice from the Australian Federal Police (AFP) to Defence of a police investigation into the origins of a military rocket launcher in the possession of criminal elements, which it believed could have been of ADF origin.[6]

4. Defence's subsequent Weapons, Munitions and Explosives Security Performance Audit (WME Audit) report was completed in August 2007.[7] The 2007 WME Audit reviewed the security policies and practices applying to Defence weapons, munitions and explosives and concluded that the culture and policies related to explosive ordnance security within Defence needed improvement. The audit made 58 recommendations, with overall responsibility for their implementation lying with the Vice Chief of the Defence Force (VCDF) Group through Joint Logistics Command (JLC).

5. Defence recognises that it needs to have a suitable system for the oversight and physical control of explosive ordnance held by ADF units, to support the effective management and control of explosive ordnance throughout its life cycle—from procurement and manufacture through to final use or disposal. Specifically, Defence's 2007 WME Audit noted that there should be an integrated system to support the end-to-end management of explosive ordnance and that, ideally, all ADF units should have access to that system for managing explosive ordnance.

6. Accordingly, it was recommended that Defence improve the policies and systems for the management and accounting of weapons, munitions and

---

5 The audit was conducted by the Defence Security Authority (DSA) under the guidance of an Oversight Board chaired by the Deputy Secretary Intelligence, Security and International Policy. The Oversight Board included representatives from relevant areas of Defence, the Australian Security and Intelligence Organisation (ASIO), and the Australian National Audit Office (ANAO) with observer status.

6 By early 2007 a joint Defence and AFP investigation confirmed that the rocket launcher was a version of an M72 short-range light anti-armour weapon disposed of by Defence some years earlier. A subsequent joint AFP and NSW Police operation resulted in charges being laid against a serving Army officer and an ex-soldier.

7 Department of Defence, Defence Security Authority, *Weapons, Munitions and Explosives (WME) Security Performance Audit*, August 2007. Defence's 2007 WME Audit was conducted in two phases, the first focusing specifically on security procedures for the M72 light anti-armour weapon and completed in January 2007. The second, broader, phase covered Defence's security policy and practice for weapons and EO security throughout the life cycle from acquisition to disposal. Unless indicated otherwise, this ANAO audit report refers to the second phase and its August 2007 report.

explosives to enhance visibility and control throughout their life cycle. Defence's progress in implementing this recommendation and other relevant 2007 WME Audit recommendations was examined during the course of this audit.

Distributing and recording explosive ordnance

7. In recent years, there have been some 75 000 movements of explosive ordnance between the explosive ordnance depots and ADF units each year.[8] The volume and type of explosive ordnance involved varies markedly, depending on the timing of major training exercises and other activities. While the volume of explosive ordnance moving through ADF units can be significant, Defence's assessment is that ADF units hold relatively small amounts in their magazines and lockers at any one time.[9]

8. Defence considers this explosive ordnance to be 'low value and less sensitive', comprising standing issues to units, along with the balance of other ordnance that has been issued to units but has not been returned to depots. This explosive ordnance is not visible through Defence's Computer System for Armaments (COMSARM). Instead, ADF units record it on Defence's general inventory management system or on other Service-specific systems.[10]

9. At the time of audit fieldwork, each Service had different arrangements in place for recording and managing explosive ordnance at the unit level. Air Force had authorised units to use COMSARM and Defence's general inventory management system, though neither system was mandated. COMSARM was available only to two Air Force units. Other Air Force units were using the general inventory management system as well as unit-level manual paper-based systems and other computer-based spreadsheets to manage their explosive ordnance transactions and holdings. Other units relied solely on unit-level systems.

---

8 Based on Department of Defence data of explosive ordnance issues and returns between ADF units and explosive ordnance depots for 2003-04 to 2009-10. This represents many thousands of pallet-loads of freight.

9 Defence informed ANAO in January 2011 that its preliminary estimate was that ADF units collectively held no more than $20 million of explosive ordnance recorded on systems outside of COMSARM.

10 COMSARM is hosted on the Defence Secret Network (DSN). Explosive ordnance items that Defence considers to be 'high value, high risk' remain visible on COMSARM after being issued to units.During the time of fieldwork for this audit, Defence's general inventory management system was the Standard Defence Supply System (SDSS). SDSS was replaced by the MILIS on 5 July 2010.

10. Army had mandated Defence's general inventory management system for unit management of explosive ordnance. In addition, some Army units also used manual paper-based systems to manage their explosive ordnance transactions and holdings. Other Army units relied solely on unit-level systems.

11. Navy required units to use an 'approved inventory management system'.[11] In practice, this included computer-based spreadsheets and paper-based inventory management systems. Additionally, Navy explosive ordnance was accounted for in COMSARM through a manual process, under which Navy units reported (via signal) all explosive ordnance transactions to a COMSARM operator, who updated COMSARM accordingly.

Previous and ongoing ANAO audit activity

12. This audit is the third in a current series of ANAO performance audits examining aspects of the major stages of management of explosive ordnance by Defence and the Defence Materiel Organisation (DMO). The major stages are:

- the identification of explosive ordnance requirements and the acquisition of the explosive ordnance, aspects of which were examined in Audit Report No.24 2009–10, *Procurement of Explosive Ordnance for the Australian Defence Force* (March 2010) and in Audit Report No.37 2009–10, *Lightweight Torpedo Replacement Project* (May 2010);
- storage of explosive ordnance at Defence explosive ordnance depots and distribution of explosive ordnance to ADF users, which is the focus of another current ANAO audit. That audit is examining Defence's management of the delivery of these services through the Explosive Ordnance Services Contract;[12]
- the sustainment or management of the explosive ordnance throughout its useful life;

---

[11] Department of Defence, Australian Book of Reference 862, Volume 2, Revision 3, Technical Manual: Maritime Explosive Ordnance Safety Manual, 19 May 2009, paragraph. 1-51 (b).

[12] Under the Explosive Ordnance Services Contract, explosive ordnance storage and distribution operations are centred on the contractor's management of 17 Defence-owned explosive ordnance storage and distribution facilities. They also include activities such as local and long haul road transport, issuing explosive ordnance to ADF units and accepting returns of explosive ordnance from ADF units, unloading imported explosive ordnance from commercial merchant vessels, and a range of repairs and scheduled maintenance.

- the management of explosive ordnance by the end users of this materiel in Defence; and
- disposal of explosive ordnance not consumed during its useful life, or otherwise declared excess or obsolete.

Audit approach

13. The objective of this audit was to examine the effectiveness of Defence's management of explosive ordnance by the end users of this materiel in Air Force, Army and Navy (the Services). In particular, the focus was on the effectiveness of arrangements for the oversight and physical control of explosive ordnance once it is issued to Service units.

14. The audit reviewed Defence's policies, procedures, processes and inventory management systems for explosive ordnance at the unit level in the ADF, from receipt and storage through to the use or return[13] of explosive ordnance. The audit also examined the relationship between the management of explosive ordnance at the unit level and the Explosive Ordnance Services Contract and, where relevant, the regional Garrison Support Services (GSS) Contracts.[14]

Overall conclusion

15. Effective control arrangements are an essential requirement for the movement and storage of explosive ordnance. Responsible authorities impose strict regulation and controls on the private and commercial transport, possession and storage of explosives to ensure that it does not create an unacceptable risk to people and property.[15] Explosive ordnance in the Defence

[13] To Defence's explosive ordnance depots which are managed by a contractor under the Explosive Ordnance Services Contract.

[14] The scope of the audit did not extend to: an assessment of the technical aspects of explosive ordnance storage and use at the unit level, including safety and occupational health and safety issues related to handling of explosive ordnance and the associated incident reporting; management of explosive ordnance in operations; examination of the management of explosive ordnance at relevant DMO managed facilities (repairs, maintenance and disposals); and base security arrangements including those managed by Defence Services Group under the regional GSS Contracts. It also did not include examination of the management of explosive ordnance at Defence explosive ordnance depots managed by a contractor under the Explosive Ordnance Services Contract. This, however, is included in the scope of another ANAO audit currently underway (see paragraph 12).

[15] See, for instance, Government of Western Australia, Department of Consumer and Employment Protection, *Storage of explosives – Dangerous goods safety guidance note X03/08*, December 2008, page 4.

domain, by its nature,[16] poses potentially higher risks to public safety and to Defence's reputation if it is mishandled or falls into the hands of those seeking to misuse it, and merits correspondingly stringent oversight and control.

16. There is an average of some 75 000 movements[17] of explosive ordnance from ADF depots to ADF units annually, representing many thousands of pallet-loads of freight. This explosive ordnance is distributed to and used by ADF units, who manage more than 800 magazines and storage lockers around Australia.[18] It is at this point that Defence's explosive ordnance becomes most dispersed, mobile and potentially vulnerable to loss or theft.

17. The sum of the explosive ordnance inventory stored in ADF units' magazines and lockers cannot be centrally scrutinised in Defence unless the ADF units holding it correctly record it on Defence's general inventory management system, MILIS.[19] However, the ANAO found ADF units that were not recording their explosive ordnance on MILIS.[20] Instead, they relied on a range of inconsistent guidance for recording and managing their explosive ordnance, using stand-alone computer-based spreadsheets and manual stock recording systems. Defence had limited assurance over ADF unit holdings, which were not subject to an effective program of monitoring and review.

18. The causes of these weaknesses in Defence's oversight and control of explosive ordnance are:

- the continuing need for ADF units to frequently process large volumes of manual explosive ordnance transactions, as Defence cannot

[16] Most of the explosive ordnance items issued to ADF units are small and portable items.

[17] Based on Department of Defence data of explosive ordnance issues and returns for 2003-04 to 2009-10.

[18] While considerable volumes of explosive ordnance can be issued to ADF units (for example, for large-scale exercises), Defence informed ANAO in February 2011 that it estimates that at other times ADF units collectively hold less than $20 million in 'low value and less sensitive' explosive ordnance, which is not material in a financial sense.

[19] During the time of fieldwork for this audit, Defence's general inventory management system was the Standard Defence Supply System, SDSS. On 5 July 2010, SDSS was replaced by the Military Integrated Logistics Information System, MILIS.

[20] Defence informed the ANAO in February 2011 that MILIS has the same functionality for the management of explosive ordnance as its predecessor SDSS. As for SDSS, to ensure that their explosive ordnance transactions are centrally visible, ADF units must manually enter their transactions onto the new general inventory management system, MILIS.

automate an interface between its key ordnance management system (COMSARM) and MILIS;[21]

- the lack of consistent and complete procedures and guidance to ADF units on recording their explosive ordnance transactions in MILIS, adding to the risks already inherent in manual processing;
- the lack of consistent guidance and instruction on the recording and reporting of explosive ordnance security incidents; and
- the lack of an effective program of monitoring and review within Defence, able to provide assurance that ADF units are completely and correctly recording their receipt, use and residual holdings of explosive ordnance in their magazines and lockers.

19. In practice, the arrangements for recording explosive ordnance transactions and holdings vary from Service to Service and within the Services, depending on the unit to which the explosive ordnance is issued. It is therefore difficult for Defence to gain assurance that all its explosive ordnance is visible and being managed in a properly controlled fashion. This difficulty was compounded by delays in MILIS achieving functionality, so that, by the end of 2010, there was a significant quantity of explosive ordnance transactions not yet entered into the system.

20. Defence informed the ANAO in February 2011 that it has embarked on a staged approach to remediating these deficiencies and making MILIS the only system on which ADF units record their explosive ordnance transactions and holdings. Defence informed ANAO that all ADF units have been directed to manually enter into MILIS their explosive ordnance holdings by 28 February 2011. Defence intends to:

- establish unit-level procedures for entering explosive ordnance holdings onto MILIS;
- by the end of 2011, develop and test, at selected ADF units, a framework for assessing unit-level procedures, so that it can obtain reliable evidence of compliance; and

[21] Defence informed the ANAO that an automated interface between COMSARM (hosted on the Defence Secret Network-DSN), and MILIS (hosted on the Defence Restricted Network-DRN), cannot be achieved without compromising the level security required for COMSARM on the DSN.

- in the longer term, withdraw COMSARM from use, so that all explosive ordnance transactions and holdings will be recorded exclusively on MILIS.[22]

21. At the unit level, the ANAO observed that Defence's policies, procedures and guidelines for the management of explosive ordnance had incomplete coverage and, in some cases, contained inconsistent advice. The gaps and inconsistencies extended from central policies and procedures, down to unit-specific instructions. The ANAO also observed inconsistencies in Defence's reporting, recording and investigation of explosive ordnance security incidents. The effect of these was to limit Defence's ability to detect, assess and mitigate its security vulnerabilities.

22. In the light of the absence of integrated systems solutions for recording explosive ordnance inventory in ADF units, and the multiple policies, procedures and guidelines applying to explosive ordnance management in ADF units, it is evident that Defence has yet to achieve oversight and assurance that all its explosive ordnance is being effectively managed at the unit level. There have been delays in implementing this core element of the recommendations of Defence's 2007 Weapons, Munitions and Explosives Security Performance Audit that were intended to achieve this end. More than three years on, Defence is only now achieving improvements to the policies and systems necessary to ensure that it achieves central visibility and control of all its explosive ordnance throughout its life cycle. The suggested actions arising from this audit aim to better position Defence to assure that its program of improvements is achieving the desired outcomes.

Key Findings

Ongoing monitoring and review at the unit level

23. Defence currently undertakes a number of ongoing reviews to inform its management of explosive ordnance and provide some assurance in relation to stock holdings. However, reviews of the management of explosive ordnance at the unit level are not well-integrated, have gaps in their coverage and do not provide an overall view of holdings or the state of controls. For example:

[22] In February 2011, Defence informed the ANAO that until such time as a single Defence inventory management and accounting system is implemented, Air Force will pursue a solution based on COMSARM to account for all explosive ordnance managed by Air Force units. Air Force intends to introduce COMSARM to all Air Force units by the end of 2011.

- While technical audits of explosive ordnance safety procedures are covered sufficiently at the unit level, there is no arrangement for counterpart audits focussing on the physical control of explosive ordnance stock holdings.
- Defence does not carry out any assurance checks of the stocktakes that ADF units are required to take of their explosive ordnance holdings.
- The findings and recommendations from all explosive ordnance audit activities at the unit level conducted by the various bodies are not centrally consolidated by Defence for monitoring, review and analysis. This limits Defence's ability to make full use of all the relevant data when identifying ongoing trends and issues in the management and physical control of explosive ordnance at the unit level in the Services.

24. The ANAO considers that there would be benefit in Defence widening the scope of its existing explosive ordnance management monitoring and review activities to include a focus on the physical control of explosive ordnance, including conducting stocktakes and business process testing at the unit level.

Managing Explosive Ordnance in ADF units

25. At the Service unit level, Defence's management of explosive ordnance relies upon multiple policies, procedures and guidelines that have gaps and inconsistencies in coverage and advice. Central oversight of Service units' explosive ordnance holdings is complicated by the Services' use of different systems to support their management tasks. These difficulties were evident at the time of Defence's 2007 WME Audit, which recommended that all publications relating to weapons, munitions and explosives management and accounting should be consolidated into an easily accessible single reference point and all obsolete security references should be removed.

26. Defence's overarching Defence Instruction General (DI(G)) on explosive ordnance management in Defence—DI(G) LOG 4-1-013 *Management of Explosive Ordnance in Defence*—has been in draft form since 2006.[23] The draft DI(G) specifies the roles and responsibilities of the authorities involved in the management of explosive ordnance in Defence. Defence informed ANAO that

[23] Defence's first recorded consideration of DI(G)) LOG 4-1-013 *Management of Explosive Ordnance in Defence* was on 5 July 2006.

in March 2011 the draft DI(G) was forwarded to the Secretary of Defence and Chief of the Defence Force for formal approval.

27. The Defence Security Manual (DSM) and Electronic Supply Chain Manual (ESCM) govern explosive ordnance security and the use of Defence's general inventory management system. In addition to these Defence-wide policy and procedure documents, Defence has single-Service policy and procedure documents dealing with the management of and accountability for explosive ordnance. These documents do not stand alone and are to be used in conjunction with other subordinate publications, instructions and manuals setting out requirements for the management of explosive ordnance. There are currently more than 600 guidance documents for managing explosive ordnance within Defence.[24] Many of the guidance documents relevant to the tracking of explosive ordnance contain outdated references to a number of other Defence publications, instructions and manuals.

28. Some areas in Defence have also created additional guidance material to supplement Defence-wide and single-Service documents, including unit-level instructions. The volume of documents addressing the physical control of explosive ordnance at the unit level, and the number of cross references between them, creates a significant challenge for Defence to maintain a suite of documentation that is relevant and reliable. Clear and up-to-date policy and procedural documentation is important to provide some assurance that there is consistency of understanding, interpretation and sound practices to support the physical control of explosive ordnance.

29. In January 2011, Defence informed the ANAO that changes made to key policy documents in late 2010 and others scheduled for release in the first half of 2011 should address the majority of the more significant issues.

Information and Records Management Systems

30. COMSARM records physical and financial data up to the point at which the explosive ordnance is issued to Service units, except where an explosive ordnance item is what Defence describes as a high cost or sensitive item that Defence has determined must be continued to be tracked in

[24] These 600 documents include all documents relating to the management of explosive ordnance including legislation, regulations, policies, standards, procurement inventory management and safety manuals and detailed work instructions. Under the Explosive Ordnance Reform Program, Defence is, undertaking the Document Management Project to rationalise the number publications related to management of explosive ordnance. This project is discussed in further detail in chapter 2 of this audit.

COMSARM until it has actually been used. The reported amount[25] of explosive ordnance inventory in Defence's financial statements is based primarily on the information held in COMSARM.

31. The annual volume of explosive ordnance issued to ADF units is considerable, particularly for units involved in large scale exercises or training. Each year, there are an average of 75 000 movements of explosive ordnance between ADF depots and units, representing several thousand pallet-loads of freight. Once explosive ordnance is issued to them it becomes the responsibility of the Service units. Units use the explosive ordnance issued to them, returning unused ordnance to depots (where it is re-entered onto COMSARM), or holding it in their unit magazines or lockers.[26]

32. Unit holdings can be recorded in Defence's general inventory management system MILIS, or in other systems including paper records, spreadsheets and other Service-specific systems. Defence does not currently have a central view of all these systems or a single system with a consolidated set of records for all explosive ordnance holdings that are not recorded in COMSARM or MILIS, notably those items issued to Service units and described by Defence as 'low value and less sensitive'.

33. Some ADF units were not recording their explosive ordnance holdings on the general inventory management system, instead managing these items on other inventory management systems such as computer based spreadsheets and manual stock recording systems. Consequently, Defence is not able to readily ascertain the quantity or physical location of all the explosive ordnance recorded in systems other than COMSARM or MILIS.

34. ANAO's findings are consistent with those of Defence's 2007 WME Audit, which found both a loss of visibility of explosive ordnance to the wider explosive ordnance domain within Defence, and a lack of clarity between the

---

[25] Defence's inventory is reported at cost, adjusted where applicable for loss of service potential. The costs of inventories are assigned by using a weighted average cost formula. Department of Defence, *Defence Annual Report 2009–10*, Volume 1, p. 214.

[26] Defence's preliminary estimate is that, at any given point in time, ADF units collectively hold no more than $20 million of explosive ordnance on systems outside of COMSARM. Defence informed the ANAO that this preliminary estimate was derived from its analysis of summary reports of 'low value and less sensitive' explosive ordnance issued to and returned from ADF units for the months of March, October and November 2010. Defence informed the ANAO that 'during these three months $30.7 million of 'low value and less sensitive' explosive ordnance was issued to ADF units and $13.9 million of 'low value and less sensitive' explosive ordnance was returned from ADF units, reflecting usage of approximately $17 million.

accounting systems used to manage explosive ordnance. The 2007 WME Audit considered this loss of visibility of explosive ordnance to be an accountability gap or 'accounting black hole' and a significant security weakness. It noted that there should be an integrated system to support the end-to-end management of explosive ordnance which, ideally, could be used by all ADF units. Defence's 2007 WME Audit recommended that Defence improve the policies and systems for the management and accounting of weapons, munitions and explosives to enhance visibility and control throughout their life cycle.

35. Pending the development of a longer-term solution to the management and control of explosive ordnance issued from COMSARM, the ANAO considers it is important that the Services develop an integrated management system to account for explosive ordnance held at the unit level. This would provide Defence-wide visibility of such explosive ordnance, and support the Vice Chief of the Defence Force in his role as the single point of accountability in Defence for explosive ordnance.[27]

36. In February 2011, Defence informed the ANAO that it is currently undertaking studies to ascertain the security and functionality requirements necessary to manage all explosive ordnance on MILIS, with the intention of moving the management of all explosive ordnance to MILIS in the future. Further Defence informed the ANAO in February 2011 that to provide more rigorous governance, it is introducing a Business Process Testing Controls Framework into the explosive ordnance domain, and that this testing will have a particular focus on explosive ordnance management by ADF units. Defence intends that the initial trial of this testing at selected Navy, Army and Air Force units will be completed by the end of 2011.

Security and Security Incident Management

37. It is important for Defence to have in place clear policies, procedures and instructions for identifying and reporting explosive ordnance security incidents and a reliable information system to manage reported incidents from initial identification through to the outcome of subsequent investigations. An effective reporting and investigation regime for explosive ordnance security

[27] The VCDF, through the CDF's Directive 4/2008, in 2008 was appointed as the single point of accountability for explosive ordnance within Defence. The VCDF has delegated this responsibility to the Commander of Joint Logistics Command (CJLOG).

incidents would inform Defence's understanding of vulnerabilities and reduce the risk of future occurrences.

38. Defence's 2007 WME Audit found that the key Defence documents describing weapons and explosive ordnance security incident requirements were inconsistent and recommended that the requirements in each be aligned. However, notwithstanding Defence's 2009 revision of key documents, ambiguities and inconsistencies remain; including important threshold definitions of what constitutes explosive ordnance security incidents, and the subsequent threshold requirements for reporting such incidents. The ambiguities and inconsistencies within and between these key documents detract from their clarity and reduce certainty for those who rely on them for guidance. This limits Defence's ability to effectively oversee and manage these types of incidents. In January 2011 Defence informed the ANAO that changes to some of Defence's key defence manuals and instructions for the management of explosive ordnance security incidents had either been completed or were in draft and that in Defence's view, these changes would address the more significant issues identified during the audit.

39. Defence's 2007 WME Audit found that Defence was not able to provide a reliable and comprehensive summary of security incidents involving weapons, munitions and explosives reflecting, in part, the disjointed system for reporting, recording and monitoring security incidents. Specific recommendations were made that policies and systems for managing and accounting for weapons, munitions and explosives be improved to enhance visibility and control of these throughout their life cycle, and that the systems (COMSARM and, at the time, SDSS) should be managed in a way that unresolved discrepancies were automatically reported to the Defence Security Authority (DSA) Security Incident Centre. Defence's 2007 WME Audit noted that these were early audit recommendations on which action had already started.

40. At the time of this audit, there was evidence that not all explosive ordnance security incidents were being promptly reported to 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 explosive ordnance security incidents, leading the ANAO to conclude that Defence has yet to achieve visibility of all explosive ordnance security incidents. In January 2011, Defence informed the ANAO that it intends to institute a system to automatically report all unresolved explosive ordnance discrepancies to DSA as part of the longer term MILIS explosive ordnance

management enhancements. Additionally, Defence informed the ANAO that Defence is now regularly reviewing the progress of explosive ordnance security incident investigations.

Recommendations

41. The ANAO has made five recommendations aimed at improving Defence's monitoring of explosive ordnance tracking arrangements at the unit level; providing an authoritative and consistent framework for the management of explosive ordnance across Defence; developing a suitable inventory management system for the Services to physically account for explosive ordnance at the unit level; and addressing limitations in the guidance, reporting requirements and data for explosive ordnance security incidents in Defence.

Summary of agency response

42. Defence welcomes the ANAO report and, while the amount of explosive ordnance held by ADF units is a small percentage of Defence's total explosive ordnance inventory, acknowledges that there is scope for further improvement in the management of explosive ordnance held by Navy, Army and Air Force. Defence agrees with all five recommendations made by the ANAO, which reflect initiatives already being pursued by Defence.

43. Defence takes its responsibility for the management and security of all explosive ordnance holdings very seriously. This is evidenced in the robust controls Defence already has in place for access to explosive ordnance including stringent requirements when custody is transferred to or from a unit and security vetting of all personnel involved in the management of explosive ordnance. Complementing this is a comprehensive regime of controls to detect any irregularities. These controls include the policy requirement for fortnightly stocktakes and regularly scheduled technical inspections. In addition, senior Defence leaders regularly review all security incidents.

44. These activities form part of an extensive program to further improve control of explosive ordnance, which is described in the 2010 Australian Defence Strategic Logistics Strategy. This program includes the promulgation of high level Defence explosive ordnance policy, and implementation of revised business processes and comprehensive business process testing in 2011. It also includes moving the management of all explosive ordnance stockholdings onto MILIS progressively, as functionality and security requirements are addressed.

Recommendations

Recommendation No.1

Para 2.18

The ANAO recommends that Defence:

(a) widen the scope of existing reviews of the management of explosive ordnance at the unit level to include a greater focus on arrangements for the physical control of explosive ordnance at the unit level including conducting a program of stocktakes or spot checks of explosive ordnance holdings at units; and

(b) consolidate the results of these reviews to facilitate monitoring of any remediation work identified as required and the analysis of emerging trends and issues at across Service units.

Defence response: *Agree.*

Recommendation No.2

Para 3.11

The ANAO recommends that, to provide an authoritative framework Defence:

(a) finalise its inaugural Defence Instruction (General) for the management of explosive ordnance; and

(b) promulgate ADF-wide advice for the management of explosive ordnance at the unit level.

Defence response: *Agree.*

Recommendation No.3

Para 4.58

The ANAO recommends that Defence develop an integrated inventory management system to account for explosive ordnance at the unit level.

Defence response: *Agree.*

Recommendation No.4

Para 5.26

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.

Defence response: *Agree.*

Recommendation No.5

Para 5.51

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

Defence response: *Agree.*

Audit Findings

1. Introduction

This chapter provides background information on explosive ordnance management arrangements within the Department of Defence (Defence), previous Australian National Audit Office (ANAO) audit reports on the management of explosive ordnance in Defence and the approach for this audit.

Background

1.1 Explosive ordnance[28] inventory in Defence has implications for the overall preparedness of the Australian Defence Force (ADF) and involves significant levels of expenditure. Additionally, the nature of explosive ordnance means that it carries unique risks, making secure storage of explosive ordnance holdings supported by reliable records even more critical. A robust and structured control environment is an essential foundation to support the effective physical control of Defence's explosive ordnance to reduce the risk of loss and provide assurance that it is available where and when it is needed.

1.2 Defence considers explosive ordnance to be 'integral to military capability and essential to the operations' of the ADF.[29]

1.3 Defence also views explosive ordnance as:

> …a valuable commodity with safety, security and shelf life attributes. Correct storage, handling and transportation practices are paramount to ensure safety, prevent loss and deterioration.[30]

1.4 Figure 1.1 illustrates the key stages in the management of explosive ordnance and the points of accountability for each stage within Defence. This audit focuses on the end use stage of the explosive ordnance life cycle. The audit scope is discussed further in paragraph 1.30.

---

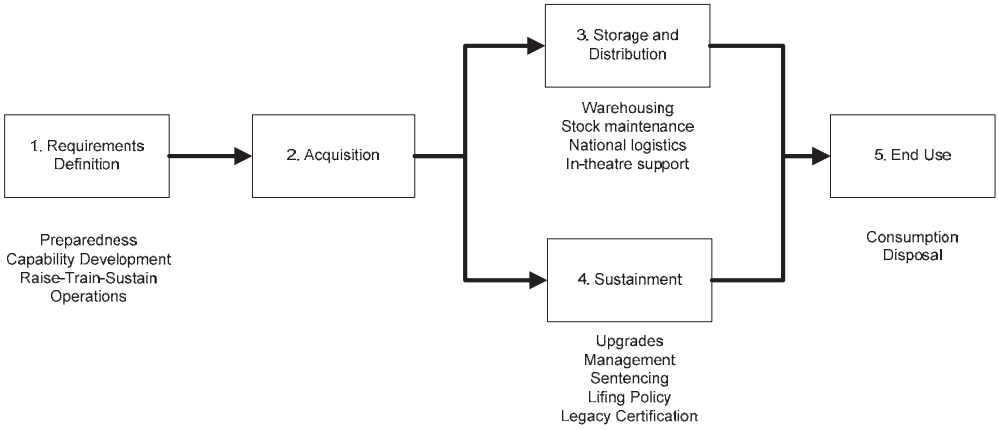
[28] The *Defence Security Manual,* 2009 states that explosive ordnance consists of all munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket and small arms ammunition; 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.

[29] Defence Policy for the Management of Explosive Ordnance, DI(G) LOG 4-1-013 (in draft).

[30] Department of Defence, 25 March 2010, *Electronic Supply Chain Manual*, V04S08C01 - Management and Accounting for Explosive Ordnance and Associated Produce, paragraph 1.

Figure 1.1

Key stages in the management of explosive ordnance in Defence

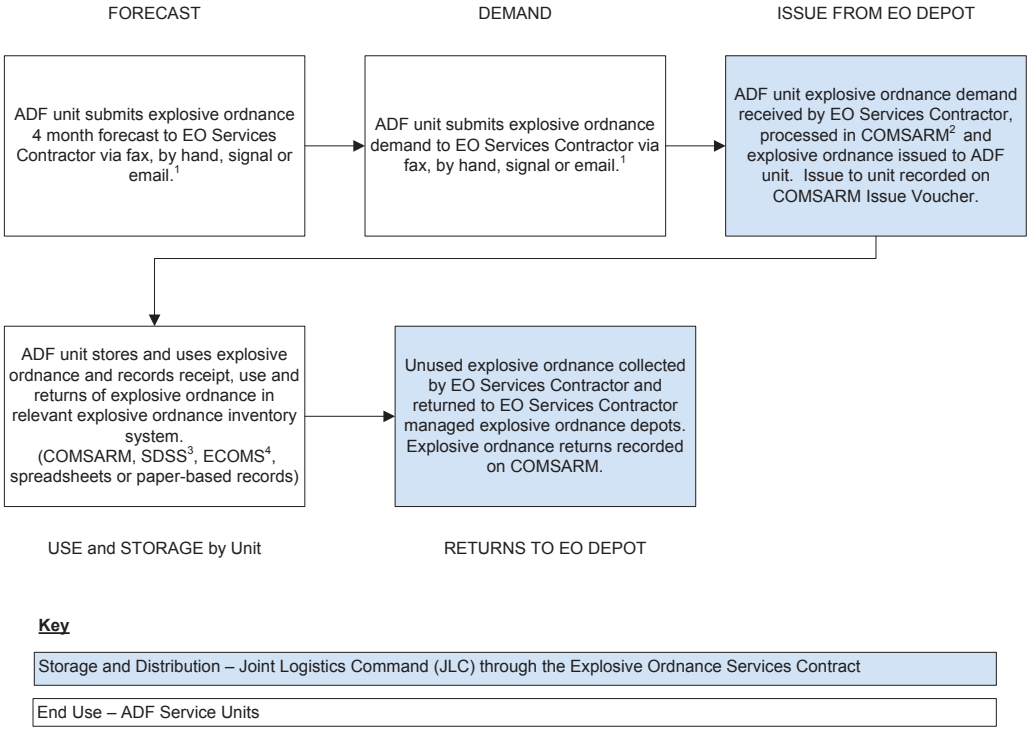


Source: Adapted from Department of Defence documentation.

1.5 Figure 1.2 provides a simplified overview of the management of explosive ordnance at the unit level in Defence.

Figure 1.2

Management of explosive ordnance at the unit level in Defence



Notes:

[1] Signals are a form of secure communication used by Navy.

[2] COMSARM (Computer System for Armaments) is Defence's primary classified explosive ordnance inventory management system.

[3] Until July 2010, the SDSS (Standard Defence Supply System) was Defence's general inventory management system that controlled the items of supply, including some explosive ordnance held at the unit level, that support the ADF and its operational capability. In the first week of July 2010, during the course of audit fieldwork for this audit, SDSS was replaced by a new logistics system the Military Integrated Logistics Information System (MILIS) through Joint Project (JP) 2077. JP 2077 consists of a number of phases. JP 2077 is managed by the DMO. In January 2011, Defence informed the ANAO that Phase 2B.1 that MILIS has the same explosive ordnance management functionality as the SDSS version it replaced.

[4] ECOMS (Explosives Custodian Officer Management System) is a classified explosive ordnance inventory management database available to Navy units.

Source: Adapted from Department of Defence documentation.

Governance arrangements

1.6 Defence's governance arrangements for explosive ordnance involve a broad range of internal and external stakeholders; internal management structures; legislative and regulatory instruments;[31] policies, procedures and activities.[32]

1.7 This audit focussed on the areas within Defence responsible for explosive ordnance management and accountability as it relates to the individual units[33] of the ADF's three Services.

1.8 Table 1.1 provides an overview of the significant stakeholders in the aspects of explosive ordnance management in Defence discussed in this audit report.

[31] Including legislation, regulations and standards which underpin Defence's key policy documents for explosive ordnance such as the Chief Executive Instructions, Defence Instructions (General) and Defence Manuals.

[32] Such as assurance, review and improvement activities; provision of subject matter expertise; promoting awareness of Defence explosive ordnance governance requirements to relevant personnel; and training.

[33] The unit level in the ADF refers to organisations within the Air Force, Army and Navy and an individual unit may consist of any number of military personnel, vehicles, ships or aircraft.

Table 1.1

Significant stakeholders in the aspects of explosive ordnance management in Defence discussed in this audit

Stakeholder	Description of responsibilities
Services – Air Force, Army and Navy	The Services (Navy,[34] Army and Air Force[35]) are responsible for the management of explosive ordnance once it has been received by their units, and during its use in training and operations.
Vice Chief of the Defence Force (VCDF)	Chief of the Defence Force (CDF) Directive number 04/2008 appointed the VCDF, through Commander Joint Logistics Group (CJLOG), as the Joint Capability Manager and single point of accountability to assure the efficient and effective management of the EO [explosive ordnance] domain.[36]
Director General Explosive Ordnance	The Director General Explosive Ordnance (DGEO) provides direct line management of the Explosive Ordnance Reform Program..The Explosive Ordnance Reform Program initiatives are outlined in paragraphs 2.20 to 2.23.
Director General Logistics Assurance	The Director General Logistics Assurance (DGLA) is accountable to CJLOG for 'providing logistics compliance and assurance, performance measurement, reporting and improvement of Defence logistics processes and systems in order to assure the effective and efficient use of logistics resources'.[37] Logistics Assurance Branch, under the DGLA, manages the Stocktake Reporting System, a repository of stocktake data of Defence assets (including inventory) managed in different systems such as ROMAN[38], COMSARM and SDSS and its replacement MILIS.
Defence Explosive Ordnance Services and Thales Australia[39]	Defence Explosive Ordnance Services (DEOS), located within JLC, manages the Explosive Ordnance Services Contract (EO Services Contract). This contract is with Thales Australia. Under the EO Services Contract, Thales Australia is responsible for transporting, storing and inspecting explosive ordnance as well as managing the distribution of explosive ordnance to meet the needs of the ADF. The relationship of the EO Services Contract with the management of explosive ordnance at the unit level is discussed in Chapter 3.

[34] Navy is also referred to as the RAN (Royal Australian Navy).

[35] Also referred to as the RAAF (Royal Australian Air Force).

[36] Department of Defence, CDF Directive 04/2008, 'Chief Of Defence Force Directive to the Vice Chief of Defence Force on Implementation of the Review of Defence Policy and Procedures for the Management of Explosive Ordnance'.

[37] Department of Defence, *The Link - Defence Logistics Magazine*, Issue 5, July 2009, p. 18.

[38] The Resource Output Management and Accounting Network (ROMAN) is Defence's financial management system.

[39] Thales Australia is a subsidiary of the Thales Group, the principal shareholders of which, at 31 December 2009, were the French Government (27 per cent) and a French company, Dassault Aviation (26 per cent).

Stakeholder	Description of responsibilities
Defence Security Authority	The Defence Security Authority (DSA) provides advice and assistance to Defence Groups and Services on protective security matters.[40] The DSA has four major roles that directly influence the management of explosive ordnance at the unit level. These are: 1. The DSA defines and promulgates the security requirements for the security of explosive ordnance in the DSM.[41] 2. The DSA provides specialist advice and assistance to areas within Defence to enable implementation of security policy. For example, the development of movement security plans and provision of threat assessments. 3. Through the Directorate of Security Performance Review (DSPR), established under the WME Program, the DSA provides ongoing review of, amongst other things, the effectiveness of the high-level risk elements of the security of explosive ordnance. 4. The Directorate of Security Intelligence and Investigations within the DSA manages the Defence Security Incident Centre (SIC) which is responsible for the assessment, referral and analysis of security incidents in Defence.
The Defence Materiel Organisation (DMO)	The DMO is the system owner of COMSARM and a number of other systems available for use within Defence to manage explosive ordnance inventory.[42] The Explosive Ordnance Division within the DMO is also responsible for managing most of the explosive ordnance marked for disposal.

Source: ANAO analysis of Defence documentation.

Defence's explosive ordnance inventory

1.9 Defence's financial statements for the year ended 30 June 2010 reported explosive ordnance inventory of $3.113 billion, consisting of over 13 000 lines and representing some 60 per cent of Defence's total reported inventory as at 30 June 2010.[43] Table 1.2 shows the reported amount of Defence's explosive ordnance inventory in Defence's financial statements, Defence's total reported

[40] Department of Defence, Defence Security Authority, Roles and Responsibilities, available from: http://www.defence.gov.au/dsa/roles_and_responsibilities/what_we_do.html> [accessed 20 April 2010].

[41] The *Defence Security Manual*, 2009 was the current version of this manual at the time of fieldwork for this audit.

[42] For example, SDSS and the Explosive Custodian Officers Management System (ECOMS) – a computerised system available to Navy units to manage explosive ordnance transactions and holdings. These systems are discussed in detail in Chapter 4 of this report.

[43] Defence's inventory is reported at cost, adjusted where applicable for loss of service potential. The costs of inventories are assigned by using a weighted average cost formula. Source: Department of Defence, *Defence Annual Report 2009–10*, Volume 1, p. 214.

inventory, and the proportion of Defence's total inventory represented by explosive ordnance at 30 June for the last three financial years.

Table 1.2

Defence's explosive ordnance inventory balances as at 30 June in the last three financial years

Year	Total Defence inventories $ million[44]	Explosive Ordnance component of total inventories $ million[45]	Explosive Ordnance as a percentage of total inventories
2007-08	4953	2828	57%
2008-09	4942	2946	60%
2009-10	5161	3113	60%

Source: Department of Defence Annual Reports.

1.10 The total explosive ordnance inventory reported in Defence's financial statements is based on the information held in COMSARM plus adjustments for some transactions not recorded in COMSARM.[46] Explosive ordnance inventory recorded in other systems used by ADF units—including Defence's general inventory management system,[47] paper records, and computerised

[44] Department of Defence, *Defence Annual Report 2008-09*, Volume 1, Appendix 9, p. 300 and Department of Defence, *Defence Annual Report 2009-10*, Volume 1, Chapter 7, p.232.

[45] ibid.

[46] Adjustments made to these figures for financial statement purposes include:

- Provision for obsolescence. Defence considers that obsolescence (technical and functional obsolescence) is the dominant factor leading to a loss of service potential of its explosive ordnance inventories. The relevant accounting standard states: 'Technical obsolescence occurs when an item still functions for some or all of the tasks it was originally acquired to do, but no longer matches existing technologies. Functional obsolescence occurs when an item no longer functions the way it did when it was first acquired.' Source: *AASB 102 Inventories*, 2009, p. 24.
- Explosive ordnance stock in transit.
- Explosive ordnance stock held on behalf of other Governments.

These adjustments are reflected in Defence's financial system as adjustments against the total explosive ordnance inventory and are not broken down by ADF Service or location.

[47] During the time of fieldwork for this audit, Defence's general inventory management system was SDSS. SDSS was replaced by MILIS on 5 July 2010.

spreadsheets—is not reflected in the total explosive ordnance inventory reported in Defence's financial statements.[48]

1.11 In the absence of a central view of all these systems, or a single system with a consolidated set of records for explosive ordnance holdings that are not recorded in COMSARM, notably those issued to Service units particularly those items issued to Service units and described by Defence as 'low value and less sensitive', Defence is not able to readily ascertain the quantity or physical location of the explosive ordnance recorded in systems other than COMSARM.

Defence's explosive ordnance inventory held by units

1.12 Defence's explosive ordnance inventory holdings are widely dispersed with Defence having approximately 840 licensed explosive ordnance storage facilities around Australia and overseas. They range from small unit magazines, lockers or safes to large explosive ordnance depot buildings. At 30 June 2008 and 30 June 2009, over 80 per cent of the unadjusted[49] amount of explosive ordnance inventory recorded in COMSARM was held at locations which, under the EO Services Contract, are managed by Defence's EO Services Contractor or at explosive ordnance facilities managed by other contractors or the DMO, with the remaining percentage being held at locations managed by ADF units. Defence informed ANAO in January 2011 that its preliminary estimate was that ADF units collectively held no more than $20 million of 'low value and less sensitive' explosive ordnance recorded on systems outside of COMSARM.

1.13 In November 2009, Defence informed the ANAO that Defence does not have a single system or consolidated set of records for explosive ordnance holdings that are not recorded in COMSARM.[50] COMSARM is rarely used directly by ADF units to account for explosive ordnance at the unit level because most ADF units do not have access to the system. Additionally,

---

[48] Except where the explosive ordnance is on the COMSARM exception listing for that Service, issued to a 'non auto-consuming' unit in COMSARM, or is issued to a Navy unit that reports explosive ordnance transactions to COMSARM operators. See Figure 4.1 in Chapter 4 for further detail.

[49] Total gross amount of explosive ordnance recorded in COMSARM was $3.2 billion at 30 June 2008 and $3.6 billion at 30 June 2009 not adjusted for, for example, provision for obsolescence and stock in transit. As noted in footnote 46, these adjustments are reflected in Defence's financial system as adjustments against the total reported explosive ordnance inventory and are not broken down by ADF Service or location.

[50] That is, explosive ordnance holdings recorded on Defence's general inventory management system, spreadsheets or other manual records.

depending on how the ADF unit and/or the explosive ordnance item is categorised in COMSARM,[51] explosive ordnance issued to an ADF unit may no longer be accounted for COMSARM, with a resulting loss of visibility to the wider explosive ordnance domain within Defence.[52] Chapter 4 discusses the various systems used within Defence to account for explosive ordnance and explains in more detail how explosive ordnance items are recorded within COMSARM once they are issued to ADF units.

Safety and security of explosive ordnance inventory

1.14 Control over explosive ordnance within the ADF has been the focus of significant internal and external scrutiny. A number of security incidents in recent years highlight the importance of effective management of the ADF's explosive ordnance inventory. Some of these incidents are listed below.

- In April 2004, the then Defence Minister confirmed investigations were underway into missing military plastic explosives and ammunition.
- In December 2006, it was reported in the media that 10 light anti-armour weapons (M72s) were stolen from the ADF between 2001 and 2003. In May 2008 an Army captain was jailed for the theft and subsequent sale of these items.
- In August 2007, an Army sergeant was jailed for the theft of weapons, ammunition, explosives and other military equipment.
- In December 2008 an M72 light anti-armour weapon was reported as stolen from the ADF in Afghanistan.
- In July 2010, it was reported in the media that 2572 rounds of assault rifle ammunition had gone missing during May 2007 in the Northern Territory and 60 rounds in Afghanistan in October 2008.
- Defence informed the ANAO that between January 2007 and January 2010:
  - 50 9 mm rounds, two 5.56 mm rounds and 800 5.56 mm blank rounds were lost in the Northern Territory (2007);

[51] The categorisation of explosive ordnance in COMSARM is discussed in further detail in Chapter 4 of this report.

[52] Defence considers this explosive ordnance to be 'low value and less sensitive'. Defence informed ANAO in January 2011 that its preliminary estimate was that ADF units collectively held no more than $20 million of 'low value and less sensitive' explosive ordnance recorded on systems outside of COMSARM.

- Three 5.56 mm rounds were stolen in the Solomon Islands (2007);
- 900 5.56 mm rounds were stolen from Defence locations in New South Wales (2008); and
- a 20 mm round was stolen from a Defence location in the Northern Territory (2009).

- In February 2011 it was reported in the media that police discovered an M72 light anti-tank weapon[53] in a house raid related to a probe into violent crime by associates of a bikie gang.
- In February 2011 it was reported in the media that police were attempting to locate an anti-personnel mine missing from the Greenbank Training Area at Greenbank in Brisbane's south following an Army exercise in late January 2011.[54]

1.15 Defence's management of explosive ordnance security incidents is discussed in more detail in Chapter 5.

Reviews and reforms of the explosive ordnance domain within Defence

1.16 In his speech to the Lowy Institute for International Policy on 10 June 2008, the then Defence Secretary noted that Defence's key reform in relation to explosive ordnance had been to streamline and strengthen accountability by making the VCDF responsible for the oversight, coordination and assurance of the efficiency and effectiveness of the overall weapons and explosive ordnance system of management. In particular, the Secretary noted that:

> ...we've also begun work on a range of activities including revising EO [explosive ordnance] accounting procedures, improving physical security at weapons and EO storage facilities, and consolidating the myriad of

[53] See 'Rocket launcher riddle', *Sunday Tasmanian*, 1st edition, p12 , Sunday, February 6, 2011. The media report stated that though the M72 light anti-tank weapon had been converted to use high-velocity training rounds, it can fire an improvised explosive device and can be re-modified to fire the rockets it was designed for. It was reported in the media that a Defence Department spokesman said attempts had been made to trace the origins of the launcher but its identification had been removed and it was not known if it had been lost or stolen.

[54] See the *Courier Mail,* February 10 2001, at <http://www.couriermail.com.au/news/police-looking-for-anti-personnel-mine-missing-after-army-exercise-at-greenbank-training-area/story-e6freon6-1226003886627> [accessed 22 March 2011].

publications in this area into a single, easily understood and accessed reference point. I should also point out that Defence industry is a critical part of the EO story, and we are working with it to improve cost and schedule performance in the EO supply chain.[55]

1.17 This statement followed a number of audits and reviews that found significant deficiencies in Defence's management of explosive ordnance. The major reviews and reforms of the explosive ordnance domain are summarised in Table 1.3, and in the following section on the Weapons, Munitions and Explosives (WME) Security Performance Audit.

Table 1.3

Significant reviews and reforms in Defence's explosive ordnance domain

Review or reform program	Description
Review of Defence Policies and Procedures for the Management of Explosive Ordnance (2007)	• The 'Review of Defence Policy and Procedures for the Management of Explosive Ordnance (EO)' (Orme Review) is an internal Defence review finalised in December 2007. • The review examined the explosive ordnance life cycle, including requirements determination, sustainment, storage and distribution and disposal. • The Orme Review found that the explosive ordnance domain was fragmented and lines of accountability unclear. • One of the main actions taken in response to the Orme Review was the appointment by the CDF of the VCDF as the single point of accountability for explosive ordnance in Defence. • In relation to the storage and distribution of explosive ordnance, the Orme Review found that the inventory management systems used by Defence were Service-specific. The review advised that the use of parallel information management systems resulted in duplication of effort in the administration of explosive ordnance. • The Orme Review also found that the lack of appropriate levels of personnel security clearances (for both Defence and contractor staff) hindered the efficiency of the distribution network.

[55] Mr Nick Warner, Secretary of Department of Defence, Speech to the Lowy Institute for International Policy, '256,800 Paper Hand Towels: Mending Defence's Broken Backbone', 10 June 2008.

Review or reform program	Description
2008 Audit of the Defence Budget	• The *2008 Audit of the Defence Budget* was a far reaching review of Defence's finances, operations and management processes. One of the objectives of the audit was to recommend to Ministers better ways to manage the Defence budget. • The audit identified a lack of clear and accurate explosive ordnance holding targets and future consumption requirements for both operational and Raise, Train, Sustain activities within Defence. • The audit also found that Defence was carrying a net overstock of explosive ordnance munitions estimated to be worth between $219 million and $247 million. • The report recommended that Defence conduct a review of munitions explosive ordnance stock to identify excess stock, cease ordering against those items until the excess is used and dispose of any remaining excess stock.
Defence White Paper 2009	• The *Defence White Paper 2009* was released on 2 May 2009. • One of the reviews underpinning the *Defence White Paper 2009* was the Logistics Companion Review, which included an explosive ordnance component. • In the Logistics Companion Review, Defence acknowledges that, in line with the findings of the 2007 Orme Review, with regard to management of explosive ordnance 'current approaches and practices are fragmented, and lack an end-to-end system perspective and single points of accountability'. • The Logistics Companion Review also states that, with regard to information systems used to manage explosive ordnance, 'The current approach to inventory management in the EO [explosive ordnance] domain is predicated on the basis that some information is classified higher than RESTRICTED [the national security classification of 'Restricted']. This drives unique systems and practices in contrast to the enterprise-level solutions that apply to other non-EO product fleets. Consequently, there is no core information node at which EO inventory can be viewed in its entirety, constraining Defence-wide management of EO'.[56] • The Logistics Companion Review recommended that, as part of Phase 2E of JP 2077 (MILIS), 'an integrated information system to support the Defence-wide management and accounting of EO be developed'.[57]

[56] Department of Defence, 2008, explosive ordnance component of the 'Logistics Companion Review to the Defence White Paper', p. 7.

[57] Department of Defence, 2008, explosive ordnance component of the 'Logistics Companion Review to the Defence White Paper', p. 8.

Review or reform program	Description
Reform of the explosive ordnance management functions led by Joint Logistics Command (2009)	• The responsibilities of the Explosive Ordnance (EO) Branch in Joint Logistics Command include: 'reviewing EO governance arrangements on a whole-of-life-cycle, whole-of-Defence basis and providing assurance of EO management through Commander of Joint Logistics Command (CJLOG) to VCDF'.[58] • The EO Branch is seeking to achieve this through the Explosive Ordnance Reform Program which was approved by CJLOG on 4 June 2009.

Source: Defence documentation.

Weapons, Munitions and Explosives (WME) Security Performance Audit (2007)

1.18 In late December 2006, the then Minister for Defence announced a security management audit of Defence weapons, munitions and explosives. This announcement followed advice from the Australian Federal Police (AFP) to Defence of a 'police investigation into the origins of a military rocket launcher in the possession of criminal elements, which it believed could have been of Australian Defence Force (ADF) origin'.[59] The audit was conducted by the Defence Security Authority (DSA) under the guidance of an Oversight Board chaired by the Deputy Secretary Intelligence, Security and International Policy.[60]

1.19 The audit report, 'Weapons, Munitions and Explosives (WME) Security Performance Audit', was completed in August 2007.[61] The 2007 WME Audit reviewed the security policies and practices that apply to Defence weapons, munitions and explosives and concluded that the culture and policies related

[58] Department of Defence, 'Explosive Ordnance Reform Program', 4 June 2009, p. 3.

[59] By early 2007 a joint Defence and AFP investigation confirmed that the rocket launcher was a version of an M72 short-range light anti-armour weapon thought to have been disposed of by Defence some years ago. A subsequent joint AFP and NSW Police operation resulted in charges being laid against a serving Army officer and an ex-soldier.

[60] The Oversight Board included representatives from relevant areas of Defence, the Australian Security and Intelligence Organisation (ASIO), and the Australian National Audit Office (ANAO) with observer status.

[61] The WME audit was conducted in two phases. The first phase of the audit focused specifically on security procedures for the M72 light anti-armour weapon. The report for phase 1 was completed in January 2007. The second phase of the audit was a broader audit covering Defence's security policy and practice for weapons and EO security throughout their life cycle from acquisition to disposal. The report for phase 2 was completed in August 2007. Except where indicated otherwise, any reference to the WME Audit in this audit report is Department of Defence, Defence Security Authority, *Weapons, Munitions and Explosives (WME) Security Performance Audit*, August 2007.

to explosive ordnance security within Defence needed improvement.[62] The audit made 58 recommendations, with overall responsibility for their implementation lying with the VCDF Group through JLC.[63]

1.20 The 2007 WME Audit included a number of findings relevant to the accountability of explosive ordnance held at ADF units. These included:

- Weaknesses in security policy and processes for explosive ordnance.
- No clear, single authority with ownership and responsibility for explosive ordnance in Defence from acquisition through to use and disposal, with confusing layers of management, processes and accountability.
- Different management systems and training programs for security personnel from each Service.
- No consolidation of explosive ordnance policy and management responsibilities, or best practice models of Defence explosive ordnance security.
- Loss of visibility of explosive ordnance to the wider explosive ordnance domain in Defence once explosive ordnance is issued to units. Visibility is lost since there is no connectivity between COMSARM (used to manage explosive ordnance at depots) and other systems used by ADF units. This loss of visibility has been referred to as accounting 'black hole'.
- Poor verification processes with the result that explosive ordnance is vulnerable to security breaches during the disposal process.

1.21 Defence's progress in implementing the recommendations from the 2007 WME Audit is discussed in Chapter 2.

---

[62] Department of Defence, 'The Review of Defence Policy and Procedures for the Management of Explosive Ordnance (EO)', 14 December 2007, Attachment B.

[63] CDF Directive 4/2008 to the VCDF, 11 March 2008.

Single point of accountability for explosive ordnance in Defence

1.22 As noted in Table 1.3, to address one of the key findings of the Orme Review,[64] the VCDF, through the CDF's Directive 4/2008,[65] was appointed as the single point of accountability for explosive ordnance within Defence. The VCDF has delegated this responsibility to the CJLOG.[66]

1.23 The Explosive Ordnance Branch was established in JLC in April 2008. The mandate for the Explosive Ordnance Branch includes 'reviewing EO governance arrangements on a whole-of-life-cycle, whole-of-Defence basis and providing assurance of EO [explosive ordnance] management through CJLOG to VCDF'.[67] The Explosive Ordnance Branch is seeking to achieve this through the Explosive Ordnance Reform Program which is discussed in paragraph 2.20.

1.24 The Explosive Ordnance Branch within JLC is also responsible for overseeing the implementation of the 2007 WME Audit recommendations. The implementation of the 2007 WME Audit recommendations in relation to accounting for explosive ordnance at the unit level is discussed further in Chapter 2 and Chapter 5.

Systems used to account for explosive ordnance inventory in Defence

1.25 Until July 2010, Defence operated two different primary systems to manage explosive ordnance inventory: COMSARM on the Defence Secret Network and SDSS on the Defence Restricted Network.[68] The Services also use a range of Service-specific inventory management systems, both computer-based and paper-based. Chapter 4 describes in further detail the systems in use to account for explosive ordnance at the unit level in the ADF.

---

64 The Orme Review found that the explosive ordnance domain was 'fragmented and lines of accountability unclear'. Source: Department of Defence, 'The Review of Defence Policy and Procedures for the Management of Explosive Ordnance (EO)', 14 December 2007, p. 2.

65 Department of Defence, Joint Logistics Command, 'Explosive Ordnance Reform Program', 4 June 2009, p. 3.

66 ibid.

67 ibid.

68 On 5 July 2010, Defence replaced SDSS with MILIS. In January 2011 Defence informed the ANAO that that MILIS has the same explosive ordnance management functionality as the SDSS version it replaced.

1.26 Defence policy and procedures for the management of explosive ordnance exist within a large collection of policy and procedural documents ranging from departmental-level manuals and Defence Instructions (within Defence's System of Defence Instructions (SoDI)[69]) through to Service-specific and unit-level guidelines. A recent Defence internal review[70] found that Defence had over 600 distinct documents[71] related to explosive ordnance, many of which were out-of-date, with overlapping or duplicated content.

1.27 Defence-wide and Service-specific procedures and policies for the management of explosive ordnance are discussed in more detail in Chapter 2 and Chapter 3.

Audit approach

1.28 This audit is the seventh ANAO audit of the explosive ordnance area in Defence since 1987.[72] The objective of the audit was to examine the effectiveness of the management of explosive ordnance by the end users of this materiel in Air Force, Army and Navy (the Services). In particular, the focus was on the effectiveness of arrangements for the physical control of explosive ordnance once it is issued to Service units.

1.29 The audit reviewed Defence's policies and procedures, and inventory management systems for explosive ordnance at the unit level in the ADF, from receipt and storage through to the use or return[73] of explosive ordnance. The audit also examined the relationship between the management of explosive

---

69 The SoDI framework consists of nine different types of policy and procedure instruments that have varying degrees of permanence, applicability and enforceability through the provisions of the *Public Service Act 1999*, the *Defence Act 1903* and the *Financial Management and Accountability Act 1997*. The nine different types are: Defence Instructions (General), Defence Manuals, Chief Executive Instructions, Single Service Instructions, Standing Instructions, Standing Orders, Departmental Instructions, Group Instructions and DEFGRAMS. Defence's SoDI is discussed further in Chapter 2 of this Issues Paper.

70 Department of Defence, Explosive Ordnance Reform Program, June 2009, paragraph 5.1.4.

71 In January 2011, Defence informed the ANAO that the list of 600 plus documents comprises all documents that may be related in any way to the management of explosive ordnance and includes legislation, regulations, policies, standards, procurement, inventory management manuals, safety manuals, and detailed work instructions.

72 The preceding six audits were: Auditor-General, Efficiency Audit Report, *Department of Defence: RAAF explosive ordnance*, December 1987; Efficiency Audit Report, *Department of Defence: safety principles for explosives*, April 1988; Audit Report No.5 1993–94, *Explosive Ordnance,* Department of Defence, September 1993; Audit Report No.8 1995–96, *Explosive Ordnance*, Department of Defence, November 1995; ANAO Audit Report No. 40, 2005–06, *Explosive Ordnance*, May 2006; ANAO Audit Report No. 24 2009–10, *Procurement of Explosive Ordnance for the Australian Defence Force*, March 2010.

73 To EO Services Contractor-managed explosive ordnance depots.

ordnance at the unit level with the Explosive Ordnance Services Contract, and, where relevant, the regional Garrison Support Services (GSS) Contract.[74]

1.30 The scope of the audit did not include an assessment of:

- procedures and processes for the management of explosive ordnance in operations;
- procedures and processes for explosive ordnance disposals.[75]
- the technical aspects of explosive ordnance storage and use at the unit level, including occupational health and safety issues related to handling of explosive ordnance and the associated incident reporting;
- the accountability of explosive ordnance at EO Services Contractor managed depots under the EO Services Contract, in operations, DMO managed facilities (repairs, maintenance and disposals); or
- base security arrangements, including those managed by DSG under the GSS Contracts.

Audit fieldwork

1.31 The explosive ordnance domain in Defence involves a range of areas in both Defence and the DMO. Fieldwork for the audit included meeting with and gathering information from staff from relevant areas including:

- Defence-appointed representatives from each of the three ADF Service Headquarters;
- JLC;
- COMSARM system managers and operators in DMO;
- Materiel Information Systems (MATIS) Branch in DMO; and
- Defence Security Authority.

[74] The scope of the audit did not extend to an assessment of the technical aspects of explosive ordnance storage and use at the unit level, including safety and occupational health and safety issues related to handling of explosive ordnance and the associated incident reporting; the accountability of explosive ordnance at EO Services Contractor managed depots under the Explosive Ordnance Services Contract, in operations, DMO managed facilities (repairs, maintenance and disposals); and base security arrangements including those managed by DSG under the regional GSS Contracts.

[75] Explosive ordnance disposals are managed by the Defence Material Organisation.

1.32 While stocktaking was not the main focus of the audit fieldwork, the audit involved an element of physical stocktaking of explosive ordnance for a number of high-risk[76] and high-volume explosive ordnance inventory.

1.33 Table 1.4 below outlines the site visits to ADF units and bases undertaken as part of the audit fieldwork.

Table 1.4

ADF units and bases visited as part of audit fieldwork

Army units and sites
• Holsworthy Barracks (2nd Commando Regiment (2CDO) and 3 Royal Australian Regiment (3RAR)) • Majura Training Area (observation of a delivery of explosive ordnance to Majura firing range by the EO Services Contractor)
Air Force bases and units
• RAAF East Sale (RAAF East Sale Combat Support Unit, Officer Training School, a number of on-base contractors that handle ADF explosive ordnance (Hawker Pacific, King, and Airflite) and Transfield (contractor that manages explosive ordnance requirements for RAAF East Sale under a Garrison Support Contract). • RAAF Amberley (Base Armament Manager (23 Squadron), 382 Expeditionary Combat Support Squadron (ECSS), 6 Squadron (F-111s), Security Police, 2 Airfield Defence Squadron (AFDS)).
Navy bases and ships
• HMAS Stirling (HMAS Stirling Base and Gunnery Department, HMAS Arunta, Navy Clearance Diving Team (CDT) 4, and representatives of the EO Services Contractor). • HMAS Manoora. • HMAS Albatross.

Source: ANAO.

1.34 Relevant findings from the unit visits are summarised in boxed blue text in the body of the audit report.

1.35 This audit was conducted in accordance with ANAO auditing standards at a cost to the ANAO of $420 000.

[76] High-risk explosive ordnance refers to explosive ordnance that is 'useful to the ill-disposed' (UID). UID is a Defence term referring to items that would be useful to criminal or extremist elements for the purpose of causing serious injury, death or destruction or items seen as attractive that could be used to create a distraction in association with other items in a criminal act, or used for less sinister purposes such as a prank.

Report structure

1.36 The remainder of this audit report is structured into four chapters:

- **Chapter 2 – Reviews and Reforms of Explosive Ordnance Management**. This chapter includes an overview of Defence's 2007 Weapons, Munitions and Explosives (WME) Security Performance Audit, the current monitoring and review of explosive ordnance at the unit level and the ongoing reforms in the explosive ordnance domain within Defence.
- **Chapter 3 – Management of Explosive Ordnance at Units**. This chapter examines Defence's framework for the management of explosive ordnance at ADF units including Defence-wide and Service-specific (Air Force, Army and Navy) policies and procedures for the management of explosive ordnance from receipt and storage through to the use or return. This chapter also examines the training available to ADF units to carry out these activities.
- **Chapter 4 – Information and Records Management Systems**. This chapter examines the various information management systems used by Defence to manage explosive ordnance. It also examines the stocktaking arrangements for explosive ordnance at the unit level in the ADF.
- **Chapter 5 – Security and Security Incident Management for Explosive Ordnance at Units.** This chapter outlines Defence's framework for explosive ordnance security and security incident reporting and investigation and discusses some explosive ordnance incident management issues from unit visits. It also discusses Defence's information management systems and data for explosive ordnance security incidents and describes some key internal reviews of explosive ordnance security within Defence.

2. Reviews and Reforms of Explosive Ordnance Management

This chapter includes an overview of Defence's 2007 Weapons, Munitions and Explosives (WME) Security Performance Audit, the current monitoring and review of explosive ordnance at the unit level and the ongoing reforms in the explosive ordnance domain within Defence.

Introduction

2.1 As discussed in Chapter 1, control over explosive ordnance within the ADF has been the focus of significant internal and external scrutiny. Additionally, a number of audits and reviews in recent years have found significant deficiencies in Defence's management of explosive ordnance. One of these, the 2007 WME Audit, followed advice from the Australian Federal Police (AFP) to Defence of a 'police investigation into the origins of a military rocket launcher in the possession of criminal elements, which it believed could have been of Australian Defence Force (ADF) origin'.[77]

Weapons, Munitions and Explosives Audit (2007 WME Audit)

2.2 As discussed in paragraphs 1.18 to 1.21, in 2007 the Defence Security Authority (DSA) completed an audit of the security policies and practices that apply to Defence weapons, munitions and explosives. The audit was conducted in two phases; the first phase covered security issues directly related to the M72 light anti armour weapon.[78] Phase 2 examined security policies and practices applying to all weapons and explosive ordnance.

2.3 The audit report for phase 2, the 'Weapons, Munitions and Explosives (WME) Security Performance Audit', was completed in August 2007[79] and

[77] By early 2007 a joint Defence and AFP investigation confirmed that the rocket launcher was a version of an M72 short-range light anti-armour weapon thought to have been disposed of by Defence some years ago. A subsequent joint AFP and NSW Police operation resulted in charges being laid against a serving Army officer and an ex-soldier.

[78] The report for phase 1 was completed in January 2007.

[79] Department of Defence, Defence Security Authority, 'Weapons, Munitions and Explosives (WME) Security Performance Audit', August 2007.

made 58 recommendations,[80] with overall responsibility for their implementation lying with VCDF through JLC.[81]

2.4 In December 2007, VCDF approved a project for the implementation of the WME Audit recommendations and requested that Heads of Groups and Services implement nominated WME Audit recommendations. In May 2009, CJLOG initiated an internal review of the WME Project (the Johnstone Review) which found that the WME Project was well administered but that it needed 'a more strategic focus, better integration, with a program rather than project view'.[82] The WME Project was subsequently restructured to strengthen the management of the project activities and reconstituted as the 'WME Security Performance Audit Implementation Program' (WME Program).[83]

2007 WME Audit findings and recommendations

2.5 The major recommendations and findings that relate to the management of explosive ordnance at the unit level are summarised in Table 2.1 below. Table 2.1 also includes information on where the relevant findings and recommendations are discussed in further detail in the remainder of this audit report.

[80] Defence subsequently categorised these recommendations as either 'major' (14), 'minor' (11), 'policy' (25), and 'other' (8) with:

- major – being WME funded projects or projects that will continue past 2009–10 financial year;
- minor – being projects expected to be closed in 2009–10 financial year;
- policy – being recommendations released on the *Defence Security Manual* (DSM), *Electronic Supply Chain Manual* (ESCM), and the Defence Explosive Ordnance Publications (DEOP); and
- other – being recommendations that fall outside of the above categories.

[81] Department of Defence, 'Weapons, Munitions and Explosive Ordnance audit establishes new capabilities in Defence', *Defence Magazine*, Issue 2 2008/09, p. 37. Available from: <http://www.defence.gov.au/defencemagazine/editions/200809_02/dsa_audit.pdf> [accessed 13 May 2008].

[82] The report made 12 recommendations to change the structure of the project to a program and to strengthen the management of the program.

[83] Department of Defence, Report on the Review of the Weapons Munitions and Explosives Project, June 2009, p. 2, paragraph 1.1.

Table 2.1

2007 WME Audit findings and recommendations relating to management of explosive ordnance at the unit level

Finding and/or recommendation	ANAO comment
Weaknesses are apparent in both security policy and processes for explosive ordnance – while Defence maintains high explosive ordnance safety standards, there is no parallel in explosive ordnance security practices.	Since 2007, the *Defence Security Manual* (DSM) has been updated. The changes to the DSM and the impact of these on units' management of explosive ordnance are discussed further in Chapter 5.
• Personnel security was an audit concern. When accounting and security processes rely on trusted individuals to undertake transactions alone, the accounting train and security systems are less reliable. • The audit made a number of physical and personnel security recommendations, including banning all unaccompanied access to explosive ordnance facilities.	During fieldwork visits to selected ADF units in the course of this audit, the ANAO examined the implementation of the updates to the DSM relating to accountability for explosive ordnance in units. These findings are discussed further in Chapter 5.
• Confusing layers of management, processes and accountability have led to uncertainty with regard to security roles and responsibilities. • The audit therefore recommended a single Defence authority to provide oversight, coordination and assurance of the overall efficiency of the weapons and explosive ordnance life cycle. • The audit also recommended a review of the roles and functions of DSA to ensure total security management across Defence.	• As noted in paragraph 1.22, the CDF subsequently appointed the VCDF, through CJLOG, as the Joint Capability Manager and single point of accountability to assure the efficient and effective management of the explosive ordnance domain in Defence.[84]

[84] Department of Defence, CDF Directive 04/2008, 'Chief of Defence Force Directive to the Vice Chief of Defence Force on Implementation of the Review of Defence Policy and Procedures for the Management of Explosive Ordnance'.

Finding and/or recommendation	ANAO comment
• The WME Audit recommended that policies and systems for managing and accounting for weapons, munitions and explosives be improved to enhance visibility and control of these throughout their life cycle, and that the accounting systems SDSS and COMSARM should be managed in a way that unresolved discrepancies were automatically reported to the DSA Security Incident Centre. • The report noted that these were early audit recommendations on which action had already started.	• Policies and procedures for the management of explosive ordnance by ADF units are discussed further in Chapter 3. • Information management systems for the management of explosive ordnance by ADF units are discussed further in Chapter 4. • Reporting of security incidents involving explosive ordnance by ADF units is discussed further in Chapter 5.
All publications relating to weapons, munitions and explosives management and accounting should be consolidated into an easily accessible single reference point and all obsolete security references should be removed.	• The Explosive Ordnance Document Management Project, which forms part of the Explosive Ordnance Reform Program, is seeking to address this finding from the WME Security Audit. This project and its current status are discussed in paragraphs 2.22 to 2.23. • Policies and procedures for the management of explosive ordnance by ADF units are discussed further in Chapter 3.
The audit recommended revised accounting procedures be introduced for explosive ordnance use in training and operations.	This recommendation related to maintaining an auditable trail for issuing one man weapon systems, such as the light anti-armour weapon, the M72. The recommendation was implemented and closed during 2008–09. Policies and procedures for the management of explosive ordnance by ADF units are discussed further in Chapter 3.
While COMSARM provides assurance of weapons and explosive ordnance accounting and security, it does not extend far enough down to give the same level of assurance at the lower levels of management.	Information management systems for the management of explosive ordnance by ADF units are discussed further in Chapter 4.
Defence has not been able to provide a reliable and comprehensive summary of security incidents involving weapons, munitions and explosives, which is a reflection of the disjointed system for reporting, recording and monitoring security incidents.	Reporting of security incidents at units involving explosive ordnance, and the data that is collected by DSA, are discussed further in Chapter 5.

Source: Department of Defence, Defence Security Authority, 'Report of the Weapons, Munitions and Explosives Security Performance Audit', 17 August 2007.

Status of the implementation of the WME Audit recommendations

2.6 In January 2011, Defence informed the ANAO that 14 WME Audit recommendations had been formally closed, closure has been requested for two recommendations, closure documentation is being prepared for four recommendations, 19 recommendations are being assessed for compliance before closure is sought and the remaining 19 recommendations are under active management by the Weapons, Munitions and Explosives Program Office.

Ongoing monitoring and review at the unit level

2.7 Defence also undertakes a number of ongoing reviews of explosive ordnance at the unit level. These include monitoring activities undertaken by the Services, audits and stocktakes undertaken by JLC, and reviews and audits undertaken by the DSA. The reviews undertaken by the DSA are discussed further in Chapter 5. The other monitoring activities and audits are discussed in more detail in the sections below.

Army monitoring at the unit level

2.8 There are two forms of monitoring which occur at the unit level in Army: the Supply Chain Assurance Framework (SCAF) and the Logistics Assurance Team (LAT). While SCAF and LAT audit teams do not focus solely on explosive ordnance within their audits, aspects of explosive ordnance management at the unit level are covered in their scope.

2.9 Army does not currently have a system for recording and monitoring the findings from the SCAF and LAT audits which could facilitate the identification of any ongoing or recurring issues in explosive ordnance management at the unit level.

Air Force monitoring at the unit level

2.10 Defence advised the ANAO in April 2010 that Air Force relies on the Explosive Ordnance Monitoring Authority (EOMA) in JLC to monitor and report compliance with the various requirements for the accountability for explosive ordnance. The role of the EOMA is discussed further in paragraphs 2.12 to 2.13.

Navy monitoring at the unit level

2.11 Navy is also audited by the EOMA. In addition, Navy also uses an audit tool known as EDMAT that was developed to capture the significant amount of data arising from the 21 individual Departmental Management Audits within a ship and to enable non-compliance and remediation activity to be tracked and trends identified. EDMAT was implemented in March 2008. In addition to Navy, the tool can also be accessed by Joint Logistics Command during annual ordnance inspections which are discussed further in paragraphs 2.12 to 2.13.

Explosive Ordnance Supply Chain Audits

2.12 JLC has regional teams that conduct annual ordnance inspections known as Explosive Ordnance Supply Chain Audits. These inspections are explosive ordnance specific technical audits that test, for example, signage, licensing, facilities management and protective grounding. Every unit with a magazine is audited annually under this program.

Explosive ordnance safety auditing

2.13 Responsibility for the auditing and monitoring of explosive ordnance safety within the ADF is shared between two elements of JLC. The Explosive Ordnance Monitoring Authority (EOMA) within the Directorate of Explosive Ordnance Services (DEOS) conducts an audit program focussed on high level explosive ordnance management and compliance with legislation and Defence Instructions. Joint Logistics Unit Explosive Ordnance Services (EOS)[85] conduct a program of ammunition and magazine inspections focussing on safety of explosive ordnance.

2.14 While EOMA and EOS audits focus primarily on safety aspects of explosive ordnance storage and usage, these audits do occasionally identify issues with the physical control and security aspects of explosive ordnance management at the unit level.

[85] JLU EOS are located regionally throughout Australia at Victoria Barracks Melbourne, HMAS Stirling, RAAF Darwin, RAAF Edinburgh Adelaide, Enogerra Brisbane, and RAAF Garbutt Townsville. They are responsible for providing explosive ordnance technical advice to all units and organizations in their region including conducting explosive ordnance monitoring audits of units.

Additional monitoring undertaken by Defence

2.15 Additionally monitoring undertaken by Defence in relation to explosive ordnance includes:

- audits of transactional files conducted by staff from DEOS to provide some assurance that correct processes and procedures have been followed, including a cross check of the statutory accounting record (COMSARM)[86] of types and quantities of selected explosive ordnance items with issues to the unit; and
- audits of the COMSARM IT Controls Framework focusing on compliance.

Opportunities to improve monitoring and review of explosive ordnance at the unit level

2.16 There are a number of issues with the monitoring and review of explosive ordnance at the unit level:

- The EOMA/EOS program provides good coverage in terms of explosive ordnance safety reviews at the unit level, however there is not a similar set of audits which focus on the physical control of explosive ordnance at the unit level.
- Defence does not carry out any assurance checks of the stocktakes that ADF units are required to take of their explosive ordnance holdings.[87]
- The information from all the reviews of the management of explosive ordnance at the unit level conducted by the various bodies is not consolidated in a central repository or database.
  - While Navy has the EDMAT tool where the results from all reviews conducted at the unit level within Navy can be captured, there is no similar tool in use in other areas of the ADF.

[86] DI(G) LOG 08-16 states that all Defence assets are to be managed on an authorized asset management system. COMSARM is authorized by DI(G) LOG 08-16, paragraph 10 that states 'specialist, sensitive and classified assets are to be managed on other authorized management systems such as Pharmaceutical Integrated Logistic System or Computer System for Armaments'.

[87] Defence requirements for stocktaking of explosive ordnance holdings at the unit level are discussed in Chapter 4.

– The results from the Army SCAF and LAT audits are presented to individual units on completion of each audit, however the results are not consolidated within a central repository or database.

2.17 This limits Defence's ability to make full use of all the relevant data when identifying ongoing trends and issues in the management and physical control of explosive ordnance at the unit level in the Services.

Recommendation No.1

2.18 The ANAO recommends that Defence:

(a) widen the scope of existing reviews of the management of explosive ordnance at the unit level to include a greater focus on arrangements for the physical control of explosive ordnance at the unit level including conducting a program of stocktakes or spot checks of explosive ordnance holdings at units; and

(b) consolidate the results of these reviews to facilitate monitoring of any remediation work identified as required and the analysis of emerging trends and issues across Service units.

Defence response

2.19 Defence agreed to the recommendation.

Reform of the explosive ordnance management functions within Defence

Explosive Ordnance Reform Program

2.20 The Defence Explosive Ordnance Committee (DEOC)[88] endorsed the Explosive Ordnance Reform Program[89] in March 2009. It was subsequently approved by CJLOG on 4 June 2009, with goal of improving the management

[88] The DEOC is a two-star advisory committee with the primary objective of supporting Commander Joint Logistics (CJLOG) (acting on behalf of the VCDF as the single point of accountability for the Defence-wide management of explosive ordnance) and Chief Capability Development Group (CCDG), as the single point of accountability for the explosive ordnance requirements to support new capability. The DEOC has representation from Chief of Joint Operations (CJOPS), Capability Development Group (CDG), the DMO, the Services and the Chief Finance Officer Group; with Defence Services Group (DSG) and Defence, Science and Technology Organisation (DSTO) as permanently invited members. The DEOC is chaired by CJLOG.

[89] Managed by the Explosive Ordnance Branch within JLC on behalf of the VCDF in his role as the single point of accountability for explosive ordnance in Defence.

of explosive ordnance in Defence. Specifically, the Explosive Ordnance Reform Program:

> …aims to establish a whole-of-life-cycle, whole-of-Defence, integrated EO [*explosive ordnance*] Governance Framework that:
>
> a) provides a management system to effectively communicate EO policy, process and procedure;
>
> b) integrates and aligns EO practices; and
>
> c) provides a means for identifying and actioning improvement opportunities.[90]

2.21 Table 2.2 outlines how Defence plans to achieve this goal and the expected outcomes of the program.

Table 2.2

Explosive Ordnance Reform Program

Actions to achieve the goal of the Explosive Ordnance Reform Program
• establish an EO Governance Framework for the development, approval, promulgation, implementation, and continual improvement of EO policy, process and procedure that is aligned with the Defence Business Model; • ensure a records management regime is maintained to provide objective evidence of conformance with the EO Governance Framework; • conduct management reviews of the EO Governance Framework and report EO performance internally and externally; • establish a risk-based conformance program to assess conformance with defined requirements and facilitate the reporting and actioning of any findings; and • ensure all personnel involved in the EO life cycle have access to, and an awareness and understanding of, the EO Governance Framework and all related EO publications and information.
Expected outcomes of the Explosive Ordnance Reform Program
• implementation of Defence Instruction (General) LOG 4-1-013 –Management of EO in Defence (currently in draft);[91] • implementation of a comprehensive and integrated EO Governance Framework; • user access to a consolidated EO 'Body of Knowledge'; • increased effectiveness and efficiency of EO management practices; and • a culture of continual improvement of EO policy, process and procedure.

Source: Department of Defence

[90] Department of Defence, Explosive Ordnance Reform Program, 4 June 2009, p. 4, paragraph 4.

[91] Defence informed ANAO in March 2011 that the draft DI(G) was forwarded to the Secretary of Defence and CDF for formal approval.

2.22 The Explosive Ordnance Reform Program includes a number of initiatives. These initiatives are described below.

- **Explosive Ordnance Governance Framework – process, policy and procedure**. This initiative aims to address the current fragmented approach to explosive ordnance within Defence, and provide users with access to a whole-of-life-cycle, whole-of-Defence view of explosive ordnance management.
- **Explosive Ordnance Performance Management.** The main focus of the Performance Management project is the development and implementation of an Explosive Ordnance Performance Measurement Framework to provide information on the effectiveness and efficiency of explosive ordnance policy, process and procedure.
- **Explosive Ordnance Training Project**. This project is intended to deliver a structured training system for the whole of Defence, improve training standards, and promote the development of a qualified and competent explosive ordnance workforce
- **Explosive Ordnance Document Management**. This project aims to identify existing explosive ordnance documents, and collate, review and rationalise explosive ordnance documentation.
- **Explosive Ordnance Website – Body of Knowledge**. The purpose of this initiative is the development of a single 'portal' for accessing all explosive ordnance related information and documentation.
- **Explosive Ordnance Incident[92] Management and Reporting Project**. This project is reviewing existing incident management and reporting policy, process and procedure, and will seek to streamline current incident management and reporting practices.

2.23 The Explosive Ordnance Incident Management and Reporting Project, and the Explosive Ordnance Training Project are scheduled for completion by the end of 2011, and early 2012 respectively. Work on the remaining initiatives is expected to continue throughout 2011.

[92] Explosive Ordnance Incidents refer to explosive ordnance safety incidents which are not in the scope of this audit. Explosive ordnance security incidents are discussed in more detail in Chapter 5.

3. Management of Explosive Ordnance at ADF Units

This chapter examines Defence's framework for the management of explosive ordnance at ADF units including Defence-wide and Service-specific (Air Force, Army and Navy) policies and procedures for the management of explosive ordnance from receipt and storage through to the use or return. This chapter also examines the training available to ADF units to carry out these activities.

Framework for the management of explosive ordnance at units

3.1 Defence policy and procedures for the management of explosive ordnance exist within a large collection of policy and procedural documents ranging from departmental-level manuals and Defence Instructions (within Defence's System of Defence Instructions (SoDI))[93] through to Service-specific and unit-level guidelines.

3.2 Clear and up to date policy and procedural documentation is important for consistency of understanding, interpretation and sound practices to support the effective management and handling of explosive ordnance. The absence of adequate guidance material increases the risks to the effective control over Defence's explosive ordnance inventory including:

- inappropriate, insufficient or excessive items being held by units;
- items not being properly recorded;
- explosive ordnance inventory items not being properly utilised and maintained; and
- unauthorised removal of items from Defence's explosive ordnance inventory.

[93] The SoDI framework is managed through the Governance and Implementation Division of the Office of the Secretary and CDF. Defence has nine different types of policy and procedure instruments which have varying degrees of permanence, applicability and enforceability through the provisions of the *Public Service Act 1999*, the *Defence Act 1903* and the *Financial Management and Accountability Act 1997*. The nine different types are: These are Defence Instructions (General), Defence Manuals, Chief Executive Instructions, Single Service Instructions, Standing Instructions, Standing Orders, Departmental Instructions and Group Instructions and DEFGRAMS.

3.3 As discussed in paragraph 1.26, Defence has over 600 distinct documents related to explosive ordnance, many of which are out of date, with overlapping or duplicated content. As noted in paragraph 2.22, Defence is attempting to address this through the EO Document Management Project[94] within the EO Reform Program. The key Defence policy documents that currently cover the physical control of explosive ordnance are discussed in paragraphs 3.4 to 3.10.

The System of Defence Instructions

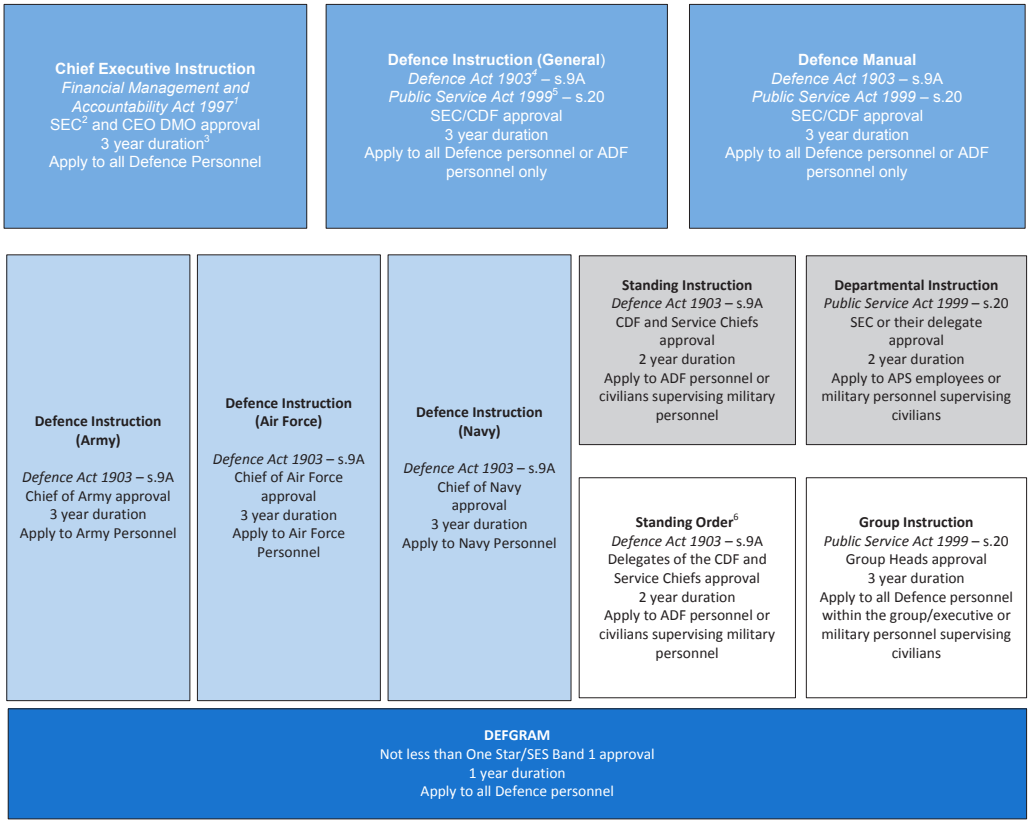
3.4 The SoDI has been the focus of significant reform since 2007.[95] The SoDI framework is managed through the Ministerial Support and Public Affairs Division of the Office of the Secretary and CDF. Figure 3.1 illustrates Defence's view of the SoDI structure.

[94] The EO Document Management Project aims to develop and implement an EO Document Management Framework; identify existing explosive ordnance documents; develop a configuration management tool to capture key data including: document, author, sponsor, release and review dates; collate, review and rationalise explosive ordnance documentation; and ensure documents have appropriate authorisation.

[95] Defence informed the ANAO that this reform has included: reform of procedures for development and approval of DI(G)s (nearing completion), update and 'de-clutter' of existing DI(G)s (completed 2010) and a review of the instruments that comprise the SoDI Framework (to be completed by mid 2011).

Figure 3.1

Defence's System of Defence Instructions



Source: Department of Defence

Note: [1] The *Financial Management and Accountability Act 1997* provides for the proper use and management of public money, public property and other Commonwealth resources, and for related purposes.

[2] Secretary of the Department of Defence.

[3] The duration of the Defence documentation is defined by Defence for administrative purposes and is not defined under the legislation.

[4] The *Defence Act 1903* is the principal Act to provide for the Naval and Military Defence and protection of the Commonwealth and of the several States.

[5] The *Public Service Act 1999* is the principal Act governing the establishment and operation of, and employment in, the Australian Public Service.

[6] Standing Orders are not specifically mentioned in DI(G) ADMIN 0-0-001, however are included in Chapter 5 of ADFP102 – Defence Writing Manual.

Defence Instructions (General)

3.5 Defence Instructions (General), commonly referred to as DI(G)s, can apply to both civilian and military personnel and may contain policy and procedure advice and instructions where compliance is mandatory and enforceable. DI(G)s are issued under section 9A of the *Defence Act 1903*. DI(G)s are always applicable to Defence members[96] and usually applicable to Defence employees.[97] DI(G)s are equivalent to general orders for the purpose of the *Defence Force Discipline Act 1982* and are reasonable directions for the purpose of the *Public Service Act 1999*.

3.6 Table 3.1 provides an overview of the key DI(G)s relevant to the physical control of explosive ordnance at the unit level in Defence at the time of ANAO audit fieldwork.

[96] Defence member, as defined in section 3 of the DFDA [*Defence Force Discipline Act 1982*] means:

(1) a member of the Permanent Navy, the Regular Army or the Permanent Air Force; or

(2) a member of the Reserves who:

(a) is rendering continuous full-time service; or

(b) is on duty or in uniform.

Source: Department of Defence, DI(G) ADMIN 0–0–001 *The System of Defence Instructions*, 26 March 2007.

[97] Defence employee means a person employed in the Department of Defence under section 22 of the *Public Service Act 1999*. Source: Department of Defence, DI(G) ADMIN 0–0–001 *The System of Defence Instructions*, 26 March 2007.

Table 3.1

Key Defence Instructions (General) relating to the physical control of explosive ordnance at units

Defence Instruction (General)	Overview of the Defence Instruction (General)
DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents*	• This DI(G) articulates the mandatory requirements for reporting and managing notifiable incidents, which includes security incidents involving explosive ordnance, in Defence.
DI(G) LOG 4-3-014 *Stocktaking of Defence Assets*	• This DI(G) requires an annual 100 per cent stocktake of ammunition and explosive ordnance, which can be a single or a progressive stocktake.
DI(G) LOG 4-1-015 *Defence Inventory Management* Governance'	• This DI(G) sets out 'an inventory management governance framework that supports the correct management and accountability'[98] of Defence logistics assets.[99] • The policy statement within this document states that 'Defence must correctly manage and account for its logistics assets to ensure availability for the preparedness of its forces, support to operations and alignment with the financial accounts'.[100]
DI(G) LOG 4-1-013 *Management of Explosive Ordnance in Defence* **(in draft)**	• This DI(G), which has been in draft form since 2006[101] was intended to identify the roles and responsibilities of the authorities involved in the management of explosive ordnance in Defence. • In ANAO Report No.24 2009–10 *Procurement of Explosive Ordnance for the Australian Defence Force*, tabled in March 2010, the ANAO reported that the draft DI(G) LOG 4-1-013 had been endorsed by the DEOC in May 2009. • Defence informed ANAO that in March 2011 the draft DI(G) was forwarded to the Secretary of Defence and Chief of the Defence Force for formal approval.

Source: ANAO analysis of Defence documentation.

---

98 Department of Defence, Defence Instruction (General) DI(G) DI(G) LOG 4-1-015 *Defence Inventory Management Governance*, 17 May 2010, paragraph 6.

99 Explosive ordnance is included in the definition of logistics assets in this Defence Instruction (General). Source: Department of Defence, Defence Instruction (General) DI(G) DI(G) LOG 4-1-015 *Defence Inventory Management Governance*, 17 May 2010, Annex A.

100 Department of Defence, Defence Instruction (General) DI(G) DI(G) LOG 4-1-015 *Defence Inventory Management Governance*, 17 May 2010, paragraph 5.

101 Defence's first recorded consideration of a draft of DI(G)) LOG 4-1-013 *Management of Explosive Ordnance in Defence* was on 5 July 2006.

Other key Defence policies and procedures for the physical control of explosive ordnance

3.7 Table 3.2 provides an overview of the key policies and procedures containing Defence's requirements, for the physical control of explosive ordnance at the unit level at the time of ANAO audit fieldwork.

3.8 In addition to Defence-wide policy and procedure documents, Defence has single-Service policy and procedure documents dealing with the management of and accountability for explosive ordnance. These documents do not stand alone and are to be used in conjunction with other subordinate publications, instructions and manuals setting out requirements for the management of explosive ordnance. The ANAO notes that as of October 2010 all these documents, last updated between 2006 and mid-2009, contain outdated references to a number of Defence publications, instructions and manuals. For example, they reference the pre-2009 version of the DSM;[102] the previous version of the Supply Chain Manual, the DSCM not the ESCM; and the pre-March 2010 version of DI(G) ADMIN 45-2.

3.9 At the Service unit level, Defence's management of explosive ordnance relies upon multiple policies, procedures and guidelines that have gaps and inconsistencies in coverage and advice. Central oversight of Service units' explosive ordnance holdings is complicated by Services' use of different systems to support their management tasks. These difficulties were evident at the time of Defence's 2007 WME Audit, which recommended that all publications relating to weapons, munitions and explosives management and accounting should be consolidated into an easily accessible single reference point and that all obsolete security references should be removed. This recommendation, while accepted by Defence, has not yet been fully implemented.[103]

[102] The *Defence Security Manual*, 2009 was the current version of this manual at the time of fieldwork for this audit.

[103] In January 2011, Defence informed the ANAO that a number of amendments had been made to the DSM in December 2010 and that these amendments are intended to consolidate specific security requirements for explosive ordnance into one reference point.

Table 3.2

Other key Defence requirements relating to the physical control of explosive ordnance at units

Policy/Procedure Document	Overview
Defence-wide documents	
Chief Executive's Instructions[104]	The two key Chief Executive's Instructions that are relevant to accountability for explosive ordnance are 6.1–Asset Management (Non-Financial Assets),[105] in which explosive ordnance is included in the definition of a Defence asset, and 6.3–Loss and Recovery of Public Property.[106]
Defence Security Manual (DSM)[107]	The primary policy document governing security for Defence personnel. and articulates, amongst other things, Defence's requirements for explosive ordnance security and the reporting and investigation of security incidents involving explosive ordnance. These requirements are discussed further in Chapter 5.
Electronic Supply Chain Manual[108]	The primary Defence Manual governing Defence supply chain operations and the use of Defence's main inventory management system, which until 1 July 2010 was the Standard Defence Supply System (SDSS).[109]
Defence Explosive Ordnance Publication 103 – Defence Explosive Ordnance Safety Manual (DEOP 103)[110]	Prescribes the policy, principles, standards and procedures for the management and safety of explosive ordnance activities in Defence.

[104] Set out the requirements for the financial management and accountability of all Defence assets and inventory in accordance with the *Financial Management and Accountability Act 1997*.

[105] Department of Defence, Chief Executive's Instructions, 6.1–Asset Management (Non-Financial Assets), 25 September 2009.

[106] Department of Defence, Chief Executive's Instructions, 6.3–Loss and Recovery of Public Property, 25 September 2009. Defence polices and procedures involving loss or theft of explosive ordnance are discussed further in Chapter 5.

[107] Department of Defence, *Defence Security Manual*, 2009 was the current version of this manual at the time of fieldwork for this audit. The DSM is a Defence Manual authorised jointly by the Secretary and the CDF under the SoDI. The DSM draws its authority from DI(G) ADMIN 20-29 *Defence Security Manual*, which was reissued during this audit on 21 May 2010.

[108] Department of Defence, 25 March 2010, *Electronic Supply Chain Manual*. The ESCM is a Defence Manual authorised jointly by the Secretary and the CDF under the SoDI.

[109] As noted in Chapter 1, in the first week of July 2010, during the course of audit fieldwork for this audit, SDSS was replaced by a new logistics system, MILIS. MILIS is discussed in more detail in Chapter 4.

[110] Department of Defence, 2003, Defence Explosive Ordnance Safety Manual (DEOP 103). DI(G) LOG 4–1–006 'Safety of Explosive Ordnance' dated 20 March 2006 provides the authority for DEOP 103.

Policy/Procedure Document	Overview
Service-specific requirements[111]	
Navy Australian Book of Reference (ABR) 862 Volume 2 Revision 3, 'Navy Technical Manual Maritime Explosive Ordnance Safety'[112]	• Navy's primary technical manual for the management of explosive ordnance. • Chapter 1 of ABR 862 details the roles and responsibilities of personnel in relation to EO [explosive ordnance] accounting. • Chapter 7 of ABR 862 provides instructions for administration of EO forecasting, demanding, receipting, returning and general accounting practice requirements for all EO embarked in naval vessels.
Army Army Logistics Procedures – 'Unit Materiel Management Procedures' (ALI POL 6-15)[113]	• The purpose of the ALI POL 6-15 is to provide unit-level materiel management policy and procedures to complement and give fidelity to the *Electronic Supply Chain Manual* (ESCM). ALI POL 6-15 covers the unit-level policy and procedures to be used by all Defence personnel for the management and accounting of materiel (asset and inventory) within the Australian Army. In all cases, the ESCM remains the senior document. • Part 3, Chapter 3 of ALIPOL 6-15 addresses explosive ordnance accounting at unit level within Army.
Air Force Australian Air Publication (AAP 3030.002) 'Air Force Supply Manual'[114]	• AAP 3030.002 articulates the unique Air Force Supply functions and states it should be used in the first instance as the point of reference for Air Force personnel. • Section 7 Chapter 1 of AAP 3030.002 provides direction for explosive ordnance (EO) accounting in Air Force and applies to all units that demand and consume EO.

Source: ANAO analysis of Defence documentation

3.10 Some areas in Defence have also created additional guidance material to supplement Defence-wide and single-Service documents, including unit-level instructions. The volume of documents addressing the physical control of explosive ordnance at the unit level, and the number of cross references between them, creates a significant challenge for Defence to maintain a suite of

[111] These documents are not stand-alone documents and state that they are to be used in conjunction with numerous other Defence publications, instructions and manuals that also contain requirements for the management of explosive ordnance.

[112] ABR 862 Volume 2 Revision 3, 'Navy Technical Manual Maritime Explosive Ordnance Safety' is issued under the authority of the Chief of Navy. The manual contributes to the Chief of Navy fulfilling his responsibilities required by DI(G) LOG 4-5-012 *Regulation of the Technical Integrity of Materiel*.

[113] The current Army specific document at the time of ANAO audit fieldwork. This publication was cancelled replaced in July 2010 following the introduction of MILIS and replaced with the Army Supply Chain Supplement incorporated within the ESCM.

[114] AAP 3030.002 is issued under DI(G) LOG 4-1-002 Electronic Supply Chain Manual.

documentation that is relevant and reliable. Clear and up-to-date policy and procedural documentation is important to provide some assurance that there is consistency of understanding, interpretation and sound practices to support the physical control of explosive ordnance.

Recommendation No.2

3.11 The ANAO recommends that, to provide an authoritative framework Defence:

(a) finalise its inaugural Defence Instruction (General) for the management of explosive ordnance; and

(b) promulgate ADF-wide advice for the management of explosive ordnance at the unit level.

Defence response

3.12 Defence agreed to the recommendation.

Requirements for units to account for explosive ordnance

Forecasting explosive ordnance requirements

3.13 To meet its contractual obligations, each month Defence requires ADF units to provide forecasts of their next three months' demands for explosive ordnance, so that the contractor is able to pre-position the required explosive ordnance at the nearest depots.[115] If explosive ordnance is not pre-positioned, the contractor cannot guarantee that demands will be met in the relevant timeframe. Failure to properly pre-position ordnance can lead to additional costs if the contractor has to arrange an unanticipated delivery of explosive ordnance. In this event, DEOS passes the additional charge on to the Service requiring the explosive ordnance.

3.14 In addition to submitting explosive ordnance forecasts in accordance with the above requirements, Navy ships must forecast known ammunitioning and de-ammunitioning requirements to the relevant explosive ordnance depot, providing the EO Services Contractor with a minimum of 28 days notice.[116]

[115] This requirement for unit forecasting does not apply to explosive ordnance required for operations. Alternative arrangements are in place for explosive ordnance for operations.

[116] In 2009–10 only 32 per cent of ammunitioning / de-ammunitioning forecasts from Navy ships met the requirement for a minimum of 28 days notice.

3.15 In 2009–10, an average of 39 per cent of actual issues of explosive ordnance had been forecast in COMSARM. Of issues that had not been forecast, the contractor was given less than 30 days notice in approximately 64 per cent of cases.[117] DEOS has raised the need for ADF units to improve their forecasting of explosive ordnance requirements with each of the Service's headquarters. The boxed text below summarises the findings from the unit visits conducted as part of the audit.

The ANAO made the following observations in regard to forecasting at the unit level in the ADF during fieldwork visits to a sample of ADF units[118]:

- **The requirement to forecast appeared not to be well known at the unit level** – ADF units visited by the ANAO were not aware of the requirement to provide a forecast of their units' explosive ordnance requirements to Defence's EO Services Contractor.
- **Some units made forecasts on an irregular basis and these could be inaccurate** –often those responsible for the management of explosive ordnance at the unit were not involved in the planning of training and exercises and were therefore unable to accurately predict and forecast the unit's future requirements,. This was particularly so in Navy units.
- **Army units had no visibility of their forecasting process** – Army units provide all their forecasts for unit exercises and training to their operations cell on a yearly basis. This information is entered into Army's primary capability planning tool, the Army Capability Management System (ACMS). The ACMS data is then consolidated at Army Headquarters to create a yearly forecast. Units, however, do not directly provide forecasts to the EO Services Contractor and were not aware whether or what information was provided to the EO Services Contractor.

3.16 There is therefore scope for ADF units to improve forecasting of their explosive ordnance requirements.

3.17 As noted in the draft report for the ANAO Performance Audit on Defence's Management of the EO Services Contract:

> These forecasts depend on ADF units' monthly forecasts of the coming quarter's demand. Ideally, they would give the contractor sufficient time to pre-position explosive ordnance at depots to meet ADF unit demands in a timely manner. In practice, the contractor was able to meet virtually all explosive ordnance demands because of its understanding of ADF units' history of explosive ordnance demands, and because the need for ADF units to provide forecasts applies to items which are in short supply. Further

[117] By ADF Service: Navy 28 per cent, Army 60 per cent, Air Force 31 per cent and Joint Operations Command 38 per cent.

[118] Two Army, eight Air Force and five Navy units were visited during audit fieldwork.

improvements are, however, unlikely to be achieved without improvements in forecasting.[119]

Explosive ordnance demands by units

3.18 Under the EO Services Contract, the EO Services Contractor is required to satisfy demands for explosive ordnance at a minimum of 14 days notice providing the explosive ordnance requirement was forecast. The contract provides for a minimum of 60 days notice for unforecast explosive ordnance demands in order to ensure explosive ordnance deliveries can be met. The satisfaction of explosive ordnance demands that have not been forecast by Service units can result in additional costs being incurred by Defence under the EO Services Contract. Where these costs are significant, Defence may pass the additional charge on to the Service requiring the explosive ordnance.

3.19 As discussed in paragraph 3.15, the majority of ADF units are falling well short of the requirements specified in the EO Services Contract for the appropriate lead time for explosive ordnance demands. Defence informed the ANAO that during 2008–09, approximately $56 030 was recovered from ADF units who had not complied with lead time requirements for explosive ordnance demands.

Receipt of explosive ordnance at units

3.20 Under the EO Services Contract, ADF units may either arrange to collect requested explosive ordnance from their supporting explosive ordnance depot or have it delivered by the EO Services Contractor to a Defence licensed explosive ordnance delivery point.[120]

3.21 Issues of explosive ordnance from explosive ordnance depots are accompanied by a COMSARM generated Issue Voucher. Relevant Defence guidance requires that, on receipt of explosive ordnance, the authorised[121] ADF unit representative is required to physically check off and sign for the delivery

---

[119] Australian National Audit Office, Performance Audit Issues Paper, Defence's Management of the Explosive Ordnance Services Contract, November 2010, paragraph 21.

[120] Such as approved areas within a Defence training/practice area, a Defence Range, a Defence Licensed Magazine or Defence Licensed Wharf, an Ammunitioning Buoy or Anchorage.

[121] The ESCM states that explosive ordnance is only to be issued to the bearer of the unit's copy of the explosive ordnance demand that has been endorsed by explosive ordnance Service Provider and a duly authorised 'Order to Draw Ammunition' form. The identity of the bearer is to be positively identified by use of a Defence ID card.

on both copies of the COMSARM Issue Voucher, ensuring that the nature, quantity and lot information listed on the COMSARM Issue Voucher are as per items received. One copy of the voucher is to be retained by the ADF unit and one copy to be retained by the depot. Units are required to use this as the accounting voucher for the explosive ordnance.

3.22 The systems, and therefore associated processes, used by ADF units to monitor the quantities and physical location of explosive ordnance from this point vary between units, primarily depending on the inventory management system in use at the unit and the extent to which the unit transactions continue to be recorded in COMSARM. The recording in COMSARM of explosive ordnance once it has been issued to units also varies, depending on the nature of the explosive ordnance being issued to the unit and the properties of the unit's identifying code in COMSARM. This is explained in more detail in Chapter 4.

Storage of explosive ordnance at units

3.23 For most units not on operations, their chief requirement for explosive ordnance is for training purposes. Defence informed ANAO that much of this explosive ordnance is used or returned to depots after a short period of time. As previously indicated, Defence informed ANAO in January 2011 that its preliminary estimate was that no more than $20 million of 'low value and less sensitive' explosive ordnance is managed by ADF units at any given point in time.

3.24 However, some ADF units do store explosive ordnance for identified future uses and are therefore required under Defence policy[122] to conduct regular stocktakes. Defence's stocktaking policies, procedures and practices are discussed further in Chapter 4.

Records of explosive ordnance holdings at units

3.25 The absence of a single mandatory system for the management and accounting of explosive ordnance held at ADF units has resulted in the development of a number of alternative manual systems and associated practices at ADF units.

[122] As discussed in Table 3.1, the Defence Instruction DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* mandates the minimum stocktake frequency for Ammunition and Explosive Ordnance as once yearly.

3.26 One method some ADF units employ to record unit holdings of explosive ordnance involves the use of manual stock cards to record the receipt, issue and balance of individual explosive ordnance items. These stock cards are generally kept with the explosive ordnance items in the relevant explosive ordnance facility. The boxed text below sets out the issues relating to the use of stock cards identified during this audit.

During the fieldwork for this audit, the ANAO found instances where the transactions recorded on such manual stock cards were not correct, for example:

- issues and returns were not being recorded on these manual stock cards and the balance of the items on hand at a particular date was determined and recorded on the card at a physical stocktake;
- totals of explosive ordnance holdings on the stock cards were incorrect due to mathematical errors; and
- instances were identified of issues and receipts of explosive ordnance having been recorded in the wrong column of the stock card (issues recorded as receipts or receipts recorded as issues) resulting in an incorrect recorded balance of explosive ordnance holdings.

3.27 Explosive ordnance holdings for Navy units are generally recorded in COMSARM.[123] In April 2010, Navy identified that as a result of a number of recent discrepancies in COMSARM, many Navy units were not aware of the stocktaking and reporting requirements for explosive ordnance. Navy has since addressed this issue by issuing a reminder to all units of the extant policies and procedures.

Returns of explosive ordnance by units to the Explosive Ordnance Services Contractor

3.28 At the completion of a unit activity, there may be surplus or unused explosive ordnance and/or produce.[124] Under the EO Services Contract, ADF units can request the EO Services Contractor to collect these items for return to an explosive ordnance depot for reissue or for disposal.[125] Requests for return

[123] While Navy units do not have direct access to COMSARM, all Navy explosive ordnance is recorded in COMSARM through a manual process whereby Navy units report via signal all explosive ordnance transactions to a COMSARM operator based at Defence Establishment Orchard Hills (DEOH) who manually inputs the relevant transactions into COMSARM. This is discussed further in paragraph 4.55.

[124] Produce includes ammunition packages, components, links, cartridge cases, etc, resulting from range practices or demolitions. Source: Department of Defence, Defence Explosive Ordnance Publication (DEOP) 103, Glossary, p.2.

[125] Relevant Defence guidance requires that prior to returning live EO, produce and packaging, ADF units are to submit an EO Return Request form detailing the EO nature, quantities being returned, date, time of return or location for collection to their supporting EO Service Provider. A copy of this form is to be retained in the EO File.

of explosive ordnance must be provided to the EO Services Contractor no less than five working days[126] prior to the required return date.

3.29 The EO Services Contractor is also contracted to collect certain range produce[127], such as brass cartridge cases, for recycling. However, the EO Services Contract does not require the EO Services Contractor to collect items that, for example:

- are classified as containing a hazardous substance;
- are not certified as being free from explosives;
- have been fired down a range; or
- have misfired.[128]

3.30 The ESCM states that the:

> EO Service Provider will not accept as returned items produce such as expended Signal Cartridges, Shot Projectiles, Smoke Grenades, Engine Starter Cartridges etc. These items are to be disposed of through local arrangements, should additional information and or clarification be required contact your local EOS [Explosive Ordnance Services] office CROO [Contract Regional Operations Officer].[129]

3.31 The disposal of explosive ordnance waste was raised with the ANAO by an Air Force unit during audit fieldwork. The issues raised are summarised below.

[126] Navy ships are also required to forecast de-ammunitioning requirements to the EO Services Contractor at least 28 days in advance of the expected de-ammunitioning date.

[127] Also known as explosive ordnance waste that has been collected at the firing point.

[128] JLC advised that this must be destroyed in situ or collected by the local JLU Explosive Ordnance Services team.

[129] Department of Defence, *Electronic Supply Chain Manual* (ESCM), Volume 4, Section 8, Chapter 1 (V04S08C01), paragraph 71.

The unit had issues with:

- the unavailability of personnel to certify items as free from explosives, with the result that the items could not be returned to the EO Services Contractor and therefore had to be stored by the unit until they could be disposed of by the unit;
- difficulties in accessing the resources required to dispose of items containing hazardous substances; and
- difficulties in accessing appropriate resources required to undertake the necessary work to destroy expended explosive ordnance before dumping (the requirement is to deface the item nomenclature and crush the container). The ANAO was informed that some Air Force units have had to place explosive ordnance items on the runway and drive over them with vehicles to comply with this requirement.

3.32 The ANAO raised the unit's concerns with DEOS. Defence subsequently informed the ANAO that the responsibility for removing range waste rests with DSG and that the relevant Air Force unit had been informed not to undertake this task. However, Defence does not have a clearly documented and agreed Defence-wide policy for managing explosive ordnance waste containing hazardous substances. In January 2011, Defence informed the ANAO that this issue will be addressed by the revision of the DI(G) 4-1-013 *Management of Explosive Ordnance in Defence* which is currently in draft form.

Contractor involvement in accounting and management of explosive ordnance at units

3.33 Garrison Support Services (GSS) describes a range of services provided to Defence sites around Australia by contractors through regionally based[130] GSS Contracts managed by Defence Services Group (DSG).[131] On some larger Defence bases, the main magazine is shared by a number of Service units and run by contractor personnel under a Garrison Support Services Contract.[132]

[130] The regions are Northern New South Wales, Southern New South Wales, Central and Western Australia, Queensland, and Victoria and Tasmania.

[131] The majority of services for which DSG is responsible are managed through three categories of regional contracts: garrison support services (GSS) contracts; comprehensive maintenance services (CMS) contracts; and recently implemented base services contracts, which combine the requirements of both the GSS and CMS contracts into a single contract. GSS refers to the activities that support ADF members and Defence civilians in their day-to-day work environment. CMS refers to the maintenance of Defence buildings and infrastructure, including fixed plant and equipment. Source: Department of Defence, Defence Support Group, 2009, *Supporting defence–a guide to doing business with Defence Support*, p 20. See ANAO Audit Report No.11 2009–10, *Garrison Support Services*, tabled in November 2009 for more information.

[132] There are often multiple units on an ADF base. In December 2010, Defence informed the ANAO that Defence has this arrangement in place at 16 Defence bases in Australia.

This was the case for one occurrence of the ADF bases visited during fieldwork for this audit.[133] This service falls under the 'management of Defence stores' category under the GSS Contract.

Training in explosive ordnance accounting available to unit personnel

3.34 The Defence Explosive Ordnance Training School (DEOTS), located at Defence Establishment Orchard Hills, was established in July 2005 and is responsible for the development of all common EO training courses and the delivery of some common Defence-wide explosive ordnance training. The DEOTS runs a number of different training courses which aim to cover different explosive ordnance competencies: from a basic introduction to explosive ordnance through to logistics, engineering and operational training.

3.35 Training at DEOTS is primarily delivered to Air Force and Navy. Explosive ordnance logistic and engineering training for Army is conducted through the Army Logistics' Training Centre.

3.36 The boxed text below highlights some of the issues related to explosive ordnance training for unit personnel identified during audit fieldwork.

- **Gaps in the training curriculum –** unit personnel interviewed during fieldwork noted that there were a number of gaps in the training provided by the DEOTS particularly in relation to the IT systems used for explosive ordnance. There was no SDSS (or now MILIS) training offered as part of the courses, and because the training offered by the DEOTS is focused on the safety and engineering aspects of explosive ordnance management, there is very little coverage of explosive ordnance accounting duties.
- **Lack of follow-up training –** a number of the units indicated that while they have received initial training in the role, there has been no follow-up or refresher training.

3.37 In October 2010, Defence informed the ANAO that the Explosive Ordnance Training Rationalisation Review – Explosive Ordnance Disposal commenced as a pilot review in January 2010 and that the results of this pilot review will result in all explosive ordnance disposal training being conducted at DEOTS in January 2012. Additionally, Defence informed the ANAO that the aim is to have all common core explosive ordnance training at a single venue by 2016.

[133] RAAF East Sale.

4. Information and Records Management Systems

This chapter examines the various information management systems used by Defence to manage explosive ordnance. It also examines the stocktaking arrangements for explosive ordnance at the unit level in the ADF.

Introduction

4.1 As identified in the explosive ordnance component of the Logistics Companion Review[134] to the *Defence White Paper 2009*,[135] Defence's ability to implement a Defence-wide approach to the management of its explosive ordnance is hindered by the fact that it does not have a central system or consolidated set of records that can provide full visibility of its explosive ordnance inventory, specifically:

> The current approach to inventory management in the EO domain is predicated on the basis that some information is classified higher than RESTRICTED [the national security classification of 'Restricted']. This drives unique systems and practices in contrast to the enterprise-level solutions that apply to other non-EO product fleets. Consequently, there is no core information node at which EO inventory can be viewed in its entirety, constraining Defence-wide management of EO.[136]

4.2 This constraint is not new and has been known to Defence for a considerable period of time. For example, ANAO Report No. 5 1993-94, *Explosive Ordnance, Department of Defence*,[137] found that the different information systems used by Services to manage explosive ordnance did not provide Defence with timely and accurate information required to effectively manage explosive ordnance holdings.

---

[134] As noted in Table 1.3, one of the reviews underpinning the *Defence White Paper 2009* was the Logistics Companion Review, which included an explosive ordnance component.

[135] Department of Defence 2009, *Defending Australia in the Asia Pacific Century: Force 2030, Defence White Paper 2009*.

[136] Department of Defence, explosive ordnance component of the Logistics Companion Review to the *Defence White Paper 2009*, paragraph 27.

[137] ANAO, September 1993, Audit Report No.5 1993-94 Efficiency Audit, *Explosive Ordnance, Department of Defence*.

4.3 Similarly, a May 2007 internal review of the management of explosive ordnance within Defence found that:

> From a logistics and financial governance perspective, managing EO in three disparate forms is not viable given the increasing focus of internal and external agencies reviewing the way in which Defence manages its inventory.[138]

4.4 The review recommended that, in order to improve the quality of information in Defence's explosive ordnance supply chain and provide 'accurate logistics, financial and operational information':

> … Defence should consider conducting a critical review of extant single service EO management procedures through a co-operative approach, including consideration of the following suggested recommendations:
>
> - Endorsing COMSARM as the sole integrated software tool for total management of EO across each Service; or
> - Developing a single system or set of procedures that are well defined, robust and meet tri-service and whole-of-Defence corporate requirements.[139]

4.5 The 2007 Orme review reported that the choice of explosive ordnance accounting system was Service-specific. Additionally, the Orme review noted that the 'existence of parallel information management systems results in duplication of efforts in the administration of explosive ordnance throughout the supply system'.[140]

4.6 The 2007 WME Audit identified gaps in managing the physical control of explosive ordnance at the unit level in Defence. Specifically the audit report identified:

- a lack of clarity between the accounting systems used to manage explosive ordnance; and
- a loss of visibility of explosive ordnance to the wider explosive ordnance domain within Defence after it is issued to Army and Air Force units due to the fact that, when explosive ordnance is issued to

[138] Department of Defence, Finance Executive, Financial Remediation – Inventory, 'An Overview of Explosive Ordnance Management in Defence', 23 May 2007, paragraph 52, p. 14.

[139] Department of Defence, Finance Executive, Financial Remediation – Inventory, 'An Overview of Explosive Ordnance Management in Defence', 23 May 2007, paragraph 53, p. 14.

[140] Department of Defence 2007, 'Review of Defence Policy and Procedures for the Management of Explosive Ordnance' (also known as the Orme Review), p. 19.

Army and Air Force units, the items are no longer recorded in COMSARM.

4.7 The 2007 WME Audit considered this loss of visibility of explosive ordnance to be an 'accounting black hole' and a significant security weakness, and that there should be an integrated system to support the end-to-end management of explosive ordnance. The audit report stated that ideally all ADF units should have access to that system for managing explosive ordnance, and recommended that Defence improve the policies and systems for the management and accounting of weapons, munitions and explosives to enhance visibility and control throughout their life cycle.[141]

4.8 The ability of Defence to make lasting improvements in the management of explosive ordnance inventory is heavily dependent on the availability of accurate and timely information from an integrated system providing full visibility of explosive ordnance holdings across the supply chain. In January 2011 Defence informed the ANAO progress reporting on the status of this recommendation to the WME Program has been suspended until Defence completes an investigation into security and functionality issues associated with the transition to a single explosive ordnance inventory management and accounting system.[142] Defence also informed the ANAO that while a firm date for full implementation of this 2007 WME Audit recommendation is yet to be established, it is expected that the implementation of the approved project strategy will be completed by 2016.

4.9 Additionally, Defence acknowledges that governance arrangements to ensure that all explosive ordnance is appropriately accounted for may not be sufficiently rigorous at this time and informed the ANAO that Defence is reviewing its current governance arrangements, with a view to introducing additional requirements, such as business process testing, to ensure that all explosive ordnance is appropriately accounted for.

---

[141] Department of Defence, Joint Logistics Command, WME Monthly Progress Report, February 2010.

[142] Defence informed the ANAO that JLC is currently pursuing two actions related to the future requirements for the management of explosive ordnance. These are:

- conducting a formal security threat assessment and risk analysis to determine the appropriate security classification of explosive ordnance related information; and
- identifying the functionality gaps between COMSARM and MILIS and determining the functionality required to develop MILIS as the single explosive ordnance inventory and accounting management system in Defence for the management of explosive ordnance.

Overview of explosive ordnance inventory management systems in Defence

4.10 Until July 2010, Defence operated two different primary systems[143] to manage explosive ordnance inventory: COMSARM on the Defence Secret Network and SDSS[144], on the Defence Restricted Network. The Services also use a range of Service-specific inventory management systems, both computer-based and paper-based. These systems are outlined in Table 4.1.

Table 4.1

Explosive ordnance inventory management systems in Defence

System	Description
Computer System for Armaments (COMSARM)	• COMSARM is the primary classified system used to account for explosive ordnance within the ADF. The primary functions of COMSARM are to: 'provide consistent inventory control for all items, total global asset visibility and reliable and complete configuration records'.[145] • COMSARM is rarely used directly by ADF units to account for explosive ordnance at the unit level because most ADF units do not have access to the system.[146]

[143] A third system known as the Lotus Notes® Intermediate Demand System (LNIDS) is a Lotus Notes based system used by some deployed ADF Force Elements (FE) to facilitate the approval of explosive ordnance demands required for operations. The management of explosive ordnance related to ADF operations falls outside the scope of this audit.

[144] Until July 2010, the SDSS was Defence's general inventory management system that controlled the items of supply, including some explosive ordnance held at the unit level, that supported the ADF and its operational capability. In the first week of July 2010, during the course of audit fieldwork for this audit, SDSS was replaced by a new logistics system MILIS.

[145] Department of Defence, 'An Overview of Explosive Ordnance Management in Defence', May 2007, p. 7.

[146] Navy record their explosive ordnance in COMSARM through a manual process which involves Navy units reporting their explosive ordnance transactions to a COMSARM operator who manually inputs the relevant transactions into COMSARM. Two Air Force bases have recently implemented COMSARM and therefore units at these bases are able to account for explosive ordnance using COMSARM.

System	Description
Standard Defence Supply System (SDSS)	• SDSS was the key logistics management system for the ADF and was in operation from the early 1990s until 5 July 2010, when it was replaced by MILIS. SDSS was an inventory management system that controlled those items of supply that support the ADF and its operational capability.[147] • Prior to July 2010, SDSS was the mandated system for Army units to record their explosive ordnance holdings. In practice, SDSS was used by some Army units to record their explosive ordnance holdings. Prior to July 2010, SDSS was the preferred system within Air Force to record explosive ordnance classified at or below the national security classification of 'Restricted'. • SDSS was replaced by MILIS on 5 July 2010. In January 2011, Defence informed the ANAO that MILIS has the same explosive ordnance management functionality as the SDSS version it replaced.
Alternative systems used at the unit level	• Defence wide policies and procedures do not mandate the use of any specific system to account for explosive ordnance at the unit level. • There are some Service-specific inventory management systems in place. For example, Navy have a classified Microsoft Access® database, the Explosives Custodian Officer Management System (ECOMS), available to Navy ships to account for explosive ordnance. • Other systems in use include computer-based spreadsheets, manual stock cards and paper files.

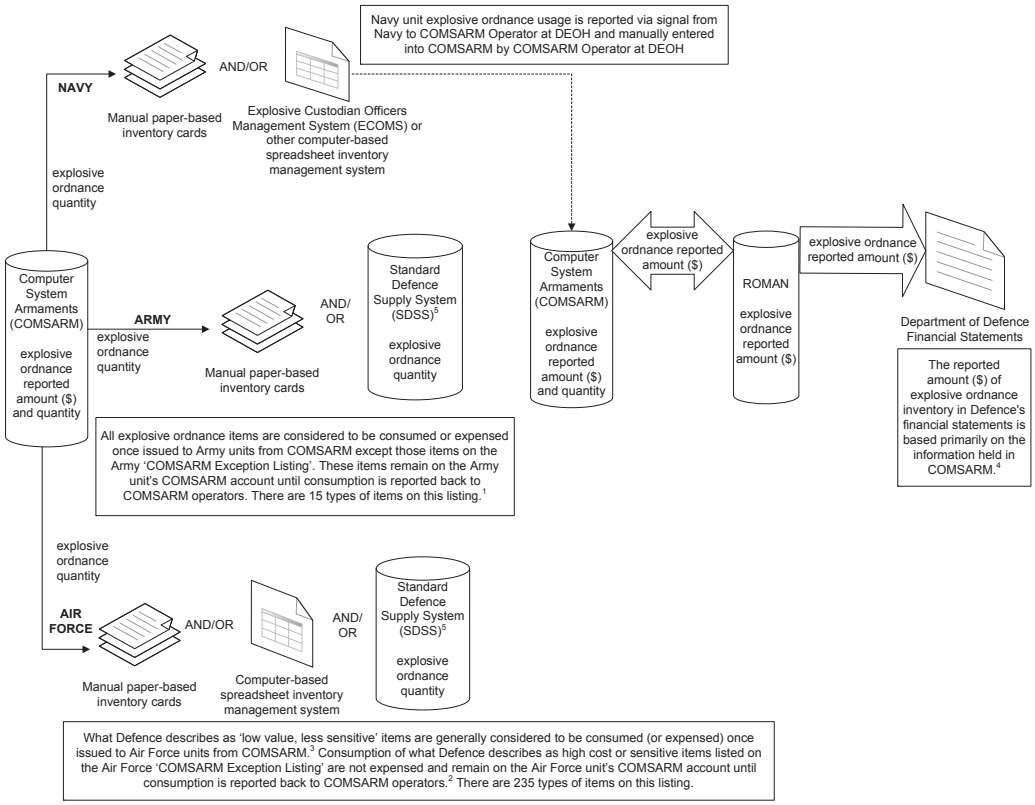
Source: ANAO analysis of Defence documentation.

4.11 Figure 4.1 illustrates the key information systems used within Defence at the time of audit fieldwork to record explosive ordnance inventory. The Services' use of these systems at the unit level is discussed in paragraphs 4.46 to 4.56.

[147] SDSS was implemented in 1993 for the Army, 1994 for the Navy, and in 1995 for the Air Force.

Figure 4.1

Key information management systems used by the Services to account for explosive ordnance (excluding operations)



Note:

1 Defence informed the ANAO in October 2010 that although there are 15 items on the 'COMSARM Exception Listing' for Army, special reporting requirements have only been promulgated for one item of this list (the M72 light anti-armour weapon). As discussed in paragraph 4.48, Defence does not have documented requirements for reporting usage of other Army 'COMSARM Exception Listing' items back to COMSARM operators.

2 At the time of audit fieldwork, Defence informed the ANAO that there are 235 types of items on the Air Force 'COMSARM Exception Listing'. As discussed in paragraph 4.50, Defence does not have documented requirements for reporting usage of such items on the Air Force 'COMSARM Exception Listing' back to COMSARM operators.

3 This is the case for units that are identified in COMSARM as 'auto-consuming' units. As noted in Table 4.2, at the time of this audit, 74 out of the 93 Air Force units identified in COMSARM were identified as 'auto-consuming' units (80 per cent). The difference between 'auto-consuming' and 'non auto-consuming' units in COMSARM is discussed further in paragraphs 4.17 to 4.21.

4 Plus, as discussed in paragraph 1.10, adjustments for some transactions not recorded in COMSARM.

5 From July 2010, SDSS was replaced by a new logistics system, MILIS, through Joint Project 2077. January 2011, Defence informed the ANAO that MILIS has the same explosive ordnance management functionality as the SDSS version it replaced.

Source: ANAO analysis of Defence documentation.

Computer System for Armaments

4.12 COMSARM was developed by Navy to provide an accountable inventory management system for the management of Navy's ammunition inventory. COMSARM was implemented in late 1988 in response to a need to control and monitor armament stores beyond the point of issue by a depot. COMSARM is managed within the Explosive Ordnance Division of the DMO at the Defence Establishment at Orchard Hills (DEOH).

4.13 As noted in Table 4.1, COMSARM is the primary system used to account for explosive ordnance within the ADF. Personnel must have a national security clearance level of 'Secret' to access COMSARM.

COMSARM use at unit level

4.14 COMSARM is used to account for explosive ordnance by two Air Force bases.[148] Air Force is currently in the process of implementing COMSARM at some key locations, with explosive ordnance items in the custody of units at RAAF East Sale and RAAF Tindal now being accounted for in COMSARM. Defence advised the ANAO that, prior to the transition to COMSARM, a full stocktake of explosive ordnance holdings at the bases was completed by Air Force staff and any variations between COMSARM records and the physical stock count were adjusted in COMSARM in consultation with the COMSARM operator at DEOH.

4.15 A small number of staff at the bases were provided with informal training on the use of COMSARM. Staff at these bases interviewed by the ANAO indicated that they considered a more formal training package would be beneficial in understanding the range of functionality of COMSARM.

4.16 In October 2010, Defence informed the ANAO that the results from the pilot implementation of COMSARM at two Air Force units will be reviewed and lessons learnt incorporated into an implementation plan to roll out the system to other major Air Force bases such as Amberley and Williamtown. Defence has yet to determine the timing for this broader implementation of COMSARM in Air Force.

[148] Some Navy and Air Force units have been provided with read-only access to COMSARM.

Categorisation of explosive ordnance in COMSARM

4.17 A Unit Designator Code (UDC) is a unique numeric code in COMSARM that is provided to all ADF units[149] that demand explosive ordnance. UDCs can be identified in COMSARM as either 'auto-consuming' or 'non auto-consuming'.

4.18 Explosive ordnance items issued from the EO Services Contractor managed explosive ordnance depots to 'non auto-consuming' units are held on the unit's UDC account in COMSARM as stock holdings until these items are either returned to an EO Services Contractor managed explosive ordnance depot (where EO Services Contractor would record their return from the unit) or they are reported to COMSARM operator at DEOH as either consumed or transferred to another unit.

4.19 Explosive ordnance items issued from the EO Services Contractor managed explosive ordnance depots to 'auto-consuming' units are considered expended upon issue and therefore not held on the unit's UDC account in COMSARM as stock holdings. The exception to this is for any items on the 'COMSARM exception listing', which is a list of the explosive ordnance that Defence considers high cost or sensitive that Defence has determined cannot be considered to be automatically consumed upon issue to a unit. At the time of this audit, Defence did not have a documented process for managing items on this listing. Defence informed the ANAO in January 2011 that the guidance for designating an item on the 'COMSARM exception listing' is in draft form in the Explosive Ordnance Supply Manual, and is planned to be published in the first half of 2011.

4.20 Items on the 'COMSARM exception listing' that are issued to an ADF unit (or any other entity in COMSARM) remain on the unit's UDC until these items are either returned to an EO Services Contractor managed explosive ordnance depot (where EO Services Contractor would record their return from the unit) or they are reported to COMSARM operator at DEOH as either consumed or transferred to another unit. Air Force has over 235 items on the COMSARM exception listing, Army has 15 items and Navy has nine items. As indicated in Figure 4.1, Air Force and Army do not have documented procedures for reporting usage of these items on the COMSARM exception

[149] As well as other entities such as DMO, other Defence entities and Defence contractors.

listing back to COMSARM operators. This is discussed in more detail in paragraph 4.48 for Army and paragraph 4.50 for Air Force.

4.21 Table 4.2 below provides the total number of units by Service identified in COMSARM in July 2010 as 'auto-consuming' or 'non auto-consuming'. It also shows the number of ADF units which were identified in COMSARM as having physical explosive ordnance holdings at that time.

Table 4.2

Units identified in COMSARM as 'auto-consuming' or 'non auto-consuming'

Service	Total no. of units by Service	Auto-consuming units	Non auto-consuming units	No. of units with explosive ordnance holdings[150]
Army	**316**	314	2	20
Air Force	**93**	74	19	33
Navy	**145**	15	130	104
TOTAL	**554**	**403**	**151**	**157**

Source: Defence Materiel Organisation

4.22 As Table 4.2 shows, most Army and Air Force units are set up in COMSARM as 'auto-consuming' units. In contrast, most Navy units are set up in COMSARM as 'non auto-consuming'.

4.23 Defence does not have a requirement for ADF units to regularly reconcile their physical explosive ordnance holdings against those recorded against their unit UDC in COMSARM.[151] This can result in incorrect stockholdings recorded in COMSARM for ADF units.

---

[150] Units with explosive ordnance holdings can be 'auto-consuming' units that have been issued items that are on the COMSARM exception listing for that Service, or 'non auto-consuming' units that have been issued any item of explosive ordnance in COMSARM.

[151] DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* requires ADF units to conduct regular physical stocktakes of explosive ordnance and reconcile their physical explosive ordnance holdings with their inventory records. However, as discussed in Table 4.1, most ADF units do not have access to COMSARM. Where items are retained on COMSARM after being issued, ADF units may be reconciling their physical holdings of explosive ordnance against single Service management records in lieu of COMSARM.

4.24 During the course of the audit, the ANAO noted a number of anomalies with the data relating to UDCs and units' explosive ordnance holdings within COMSARM. These include:

- The ANAO was provided with a list from COMSARM of explosive ordnance holdings by UDC, including the UDC's location. The ANAO asked for more detail from Defence on the explosive ordnance items held by a UDC located in the ACT which was listed as having explosive ordnance holdings. Subsequently, Defence informed the ANAO that a check of the UDC showed one item of explosive ordnance that had been issued to that UDC had actually been issued to another UDC located in NSW.
- Navy has commenced a review of Navy UDCs in COMSARM.[152] The ANAO was informed that there were approximately 1100 Navy UDCs, of which around 75 per cent have now been deactivated. Navy informed the ANAO that these deactivated UDCs had no explosive ordnance holdings recorded in COMSARM; and, as part of the review, Navy will determine how many additional UDCs should be deactivated, and the number of UDCs requiring deactivation that are currently holding explosive ordnance stock. Navy subsequently informed ANAO that these items of stock will either need to be accounted for or written off before the UDCs can be deactivated.

4.25 The ANAO suggests that Defence:

- conducts a review and clean up of data held against all ADF unit UDCs in COMSARM to verify that each UDC represents an existing unit, the UDCs are correctly identified as either 'auto-consuming' or 'non auto-consuming' units and that the explosive ordnance holdings recorded against each UDC are correct;
- review the COMSARM exception listing for each Service to make sure it is up to date and correctly reflects the explosive ordnance items Defence considers is necessary to have full visibility of throughout their life cycle; and

[152] Navy advised the ANAO that this review was prompted by the use of a COMSARM UDC by a unit other than the UDC 'owner' when placing a request for explosive ordnance. This was identified by the COMSARM operator at DEOH who recognised that the unit requesting the explosive ordnance against that UDC was not the UDC 'owner' and was located in another state.

- implement a coherent and appropriately documented set of policies to maintain the integrity of the explosive ordnance inventory data within COMSARM related to ADF unit explosive ordnance holdings.

Standard Defence Supply System

4.26 SDSS was the key logistics management system for ADF from the early 1990s until July 2010.[153] SDSS was implemented in 1993 for Army, 1994 for Navy and in 1995 for Air Force. The system underwent a major upgrade commencing in November 2000, known as the SDSS Upgrade Project, which resulted in the release of a new version of SDSS in July 2003.[154] This was followed by a DMO-initiated Get Well Programme, and subsequently, other related programs to remediate outstanding issues relating to system performance.[155]

4.27 A January 2008 report from a project to examine solutions for end-to-end visibility and management of explosive ordnance in Defence,[156] identified a number of limitations in the ability of SDSS to provide the necessary support to users for the management of explosive ordnance including:

a. [a lack of] support of ADF policy on EO management, for example the Army's Ammunition Field Accounting manual. This includes manual processes such as the use of form SQ97 "Supply Unit Internal

[153] The Joint Committee for Public Accounts and Audit (JCPAA), JCPAA Report 317 'A champagne appetite but only a beer income-Defence's Supply Systems Redevelopment Project', of 1992 covered the development of the original SDSS product.

[154] In August 2004, the ANAO tabled a report into the management of the SDSS upgrade, ANAO Audit Report No. 5 2004–05, *Management of the Standard Defence Supply System Upgrade*. This report found that the project did not deliver value for money to Defence, exhibited extensive scope reduction and operated with an extended schedule in excess of 200 per cent of the planned schedule. The audit concluded that the project had failed to materially deliver many of the outcomes for which it was funded. This report was subsequently reviewed by the Joint Committee for Public Accounts and Audit (JCPAA) with the resulting Committee's report, JCPAA Report 404 'Review of Auditor-General's Reports 2003–2004 Third & Fourth Quarters; and First and Second Quarters of 2004–2005' published in October 2005.

[155] The DMO Get Well Programme was the subject of ANAO Audit Report No.10 2006–07, *Management of the Standard Defence Supply System Remediation Programme*.

[156] CJLOG Directive 01/07 JLG/OUT/2007/208, dated 12 Feb 2007, directed that action be taken to address explosive ordnance tracking and deployed management issues and to formulate solutions for end–to–end visibility and management of explosive ordnance within Defence. This directive resulted in a project office being established within the Materiel Information Systems Branch (MATIS) of the DMO to scope the requirements for enhanced IT support to enable end-to-end visibility and tracking of explosive ordnance in Defence. The resulting project was initially known as the COMSARM Operational Visibility Enhancement (COVE) project. The stated limitations of SDSS come from the Operational Concept Document for the COVE Capability, COVE Project Office, Document Number: MATIS 03/11/10, Version: 1.01, 25 January 2008, p. 4.

Ammunition Examination and Movement Order". There is no cross reference between the mandated physical documentation and SDSS.

b. [SDSS has] no information fields on user constraints.

c. [SDSS has] no detail on Net Explosive Quantity so that ammunition is stored in accordance with prescribed safety standards.

d. [SDSS] is not able to block the storage of incompatible natures of ammunition in the same site.

e. SDSS cannot print full item names on documentation to facilitate visual inspection / checking of consignments. This makes accurate receipt and issue at unit level extremely difficult.

f. SDSS has no facility for management of technical integrity issues such as changes in shelf life due to replacement of subcomponents on complex EO, such as the propulsion system of a guided missile.[157]

Joint Project 2077 Military Integrated Logistics Information System

4.28 The limitations of SDSS described in paragraph 4.27 above were expected to be rectified by Joint Project 2077 Military Integrated Logistics Information System (MILIS). Joint Project 2077 is a multi-phased project that seeks to improve Defence's logistics information systems through the implementation of MILIS. According to the DMO, Joint Project 2077 is to deliver:

> …a single logistic information system to enable end-to-end management of Defence's integrated supply chain. MILIS is designed to support logistic processes for Australian Defence Force (ADF) units and headquarters in barracks and in the field. This includes support to deployed forces operating in locations with interrupted communications and will lay the foundation for improved financial management, integrated supply, inventory management, maintenance, movements and distribution throughout the ADO [Australian Defence Organisation].[158]

4.29 According to Defence, MILIS is a commercial-off-the-shelf (COTS) Mincom-developed product. In January 2011, Defence informed the ANAO

[157] Department of Defence, 'Operational Concept Document for the COMSARM Operational Visibility Enhancement (COVE) Capability', Draft, 25 January 2008, pp. 4-5, paragraph 6.

[158] Defence Materiel Organisation, Projects, Joint Project (JP) 2077 - Logistics for the Warfighter, Building a world-class Military Integrated Logistics Information System, available from <http://www.defence.gov.au/dmo/coo/jp2077/index.cfm> [accessed 11 May 2010].

that Phase 2B.1 of MILIS has the same explosive ordnance management functionality as the SDSS version it replaced. MILIS went live on 5 July 2010.

4.30 Enhancement of the explosive ordnance functionality of MILIS has experienced schedule slippage as indicated below:

- In mid 2007, Phase 2D of the project was to include information capabilities that enhanced the management of explosive ordnance. It was also intended to include functionality to enable MILIS to operate on the Defence Secret Network. Second Pass Approval by Government for Phase 2D was scheduled for the end of 2008 with the intention that the capabilities would be rolled out in Defence in blocks of systems between 2010 and 2014.
- In March 2008, Defence noted that Phase 2D of the project originally included enhanced explosive ordnance functionality which had now been removed, and that MILIS was likely to gain enhanced explosive ordnance functionality in Phase 2E of the project, expected to be implemented in 2014.
- The explosive ordnance component of the Logistics Companion Review to the *Defence White Paper 2009* noted that Defence's required future explosive ordnance functionality was to be included in Phase 2E of JP 2077 and that this was not in the current *Defence Capability Plan*.[159] Consequently, Phase 2E of JP 2077 is not being progressed.
- In January 2011, Defence informed the ANAO that the inclusion of enhanced explosive ordnance functionality in MILIS is a potential option that will be considered when currently studies to clearly define the security and functionality requirements are completed in 2011.

4.31 Defence is currently working on identifying the functionality gaps between COMSARM and MILIS and determining the functionality required to develop MILIS for the management of explosive ordnance. Defence informed the ANAO in February 2011 that it has embarked on a staged approach to achieve the goal of making MILIS the only system on which ADF units record their explosive ordnance transactions and holdings. Defence informed ANAO

[159] The Defence Capability Plan provides an account of Major Capital Equipment proposals that are currently planned for Government consideration (either first or second pass approval).

that all ADF units have been directed to manually enter into MILIS their explosive ordnance holdings by 28 February 2011. Defence intends to:

- establish unit-level procedures for entering explosive ordnance holdings onto MILIS;
- by the end of 2011, develop and test, at selected ADF units, a framework for assessing unit-level procedures, so that it can obtain reliable evidence of compliance; and
- in the longer term, withdraw COMSARM from use, so that all explosive ordnance transactions and holdings will be recorded exclusively on MILIS.[160]

Stocktaking of explosive ordnance at units

4.32 The United Kingdom's National Audit Office 2007 guide *IPSAS – Preparing for Audit* provides advice to organisations on how to prepare accounts which are capable of withstanding audit scrutiny. The guide states the following in relation to stocktaking:

> To provide assurance that the balances held in the inventory system are accurate, it is important that the entity establishes a programme of regular stocktakes. The majority (by value) of inventory items should be covered by an annual stocktake at the period end. However, where entities hold significant balances of inventory, it may be more appropriate to develop a cyclical stock programme, whereby inventory items are counted on a regular basis (with the majority counted each year), but not necessarily all at the period end.[161]

4.33 The guide also notes that 'it is important that all discrepancies, identified during stocktaking, are recorded and actioned accordingly'[162] and that 'recording the discrepancies will help identify trends and allow future action, as appropriate, to limit losses'.[163]

---

[160] In February 2011, Defence informed the ANAO that until such time as a single Defence inventory management and accounting system is implemented, Air Force will pursue a solution based on COMSARM to account for all explosive ordnance managed by Air Force units. Air Force intends to introduce COMSARM to all Air Force units by the end of 2011.

[161] UK National Audit Office, *IPSAS – Preparing for Audit*, 2007, p. 18.

[162] ibid.

[163] ibid.

4.34 As noted in paragraph 3.23, for most units not on operations the chief requirement for explosive ordnance is for training purposes. Defence informed ANAO that ADF units hold relatively little in their magazines and lockers at any one time. However, some ADF units do store explosive ordnance for identified future uses and are therefore required under Defence policy to conduct regular stocktakes.[164]

4.35 Defence Instruction (General) Logistics 4-3-014 *Stocktaking of Defence Assets*, promulgated in 2005 and current at the time of the audit, outlines the requirements for stocktaking of Defence assets, including explosive ordnance. The Defence Instruction notes the importance of a robust stocktaking program:

> Through an effective stocktake program, management can be assured that the Defence asset registers reflect actual physical holdings and applicable item tracking reference data. Failure to accurately record asset holdings and applicable item tracking reference data may result in inaccurate preparedness levels and Defence financial statements, poor logistics decisions in support of operations and incorrect performance reporting.[165]

4.36 The Defence Instruction requires that stocktaking of explosive ordnance must take place at least once a year and that the '100 per cent stocktake can be either a single or a progressive stocktake'.[166]

4.37 All unit commanders are required to maintain a stocktake register that must, at a minimum, contain:

> stocktake type and number, storage locations, and the number of stock codes counted, the quantity and value of any unlisted or deficient adjustments, start and end dates for the stocktake, and the error rate percentage by stock code and value. [167]

4.38 The Defence Instruction also requires Unit Commanders/Managers:

> to ensure that personnel independent of daily warehousing/stock management and custodial functions should conduct spot-checks. [168]

---

[164] As discussed in Table 3.1 the Defence Instruction DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* mandates the minimum stocktake frequency for Ammunition and Explosive Ordnance as once yearly.

[165] Defence Instruction (General) Logistics 4-3-014 *Stocktaking of Defence Assets*, p. 1.

[166] ibid, p. 3.

[167] ibid, p. 6.

[168] ibid, p. 7.

4.39 The DSM states that spot-checks of explosive ordnance within Defence must occur on at least a monthly basis:

> Periodic, cyclic (minimum monthly) and special spot-checks of stocks must be conducted to augment security measures.
>
> … Any discrepancies must be reported as a security incident to the DSA Security Incident Centre (SIC) in accordance with DSM Part 2:67 Explosive Ordnance Security, paragraph 67.60.[169]

4.40 The reporting of security incidents in relation to explosive ordnance is discussed in more detail in Chapter 5.

4.41 Table 4.3 below provides further information on the stocktaking of explosive ordnance at the unit level including the Service-specific instructions and procedures.

Table 4.3

Instructions and procedures for stocktaking explosive ordnance by ADF Service

Army	Air Force	Navy
• ESCM states explosive ordnance stocktakes must be undertaken annually. This 100 per cent stocktake can be either single or progressive. 100 per cent fortnightly checks must also be undertaken. • Army's key guidance policy on explosive ordnance accounting states fortnightly checks must be undertaken, and checks are to be recorded on Unit Security Register.	• Air Force's key policy document on explosive ordnance accounting states that 100 per cent stocktake must be conducted annually of explosive ordnance and the results recorded on the Stocktake Reporting System (SRS). • Explosive ordnance holdings must also be verified by 100 per cent fortnightly stock check.	• Navy's key policy document on explosive ordnance accounting states that a 100 per cent muster of explosive ordnance holdings must occur every month. • Explosive ordnance musters must be conducted by a person independent of the issue of explosive ordnance. • The results of all musters are to be included in the Explosive Accounting Officer and Ship's Explosive Ordnance Safety Officer Log.

Source: Defence documentation.

[169] Department of Defence, *Defence Security Manual*, 2009, Part 2:67, Annex B – Storage of Explosive Ordnance, paragraphs 6-7.

Range of definitions in Defence-wide and Service-specific policies and procedures

4.42 There are a range of definitions within the Defence-wide and Service-specific manuals in relation to the stocktaking of explosive ordnance at the unit level. The ANAO has identified the following inconsistencies in regard to the various manuals, policies and procedures:

- Various terms are used to describe the checks of explosive ordnance that should be undertaken at the unit level, and many of these terms are not defined in the relevant policy document. For example, Defence Instruction (General) Logistics 4-3-014 *Stocktaking of Defence Assets*[170] refers to 'stocktakes' and also refers to 'spot checks' although the latter term is not defined in the DI(G). It is not clear whether a 'spot check' is a sighting or a stocktake of a percentage of explosive ordnance held. Army and Navy policies refer to 'checks' and 'musters' respectively.[171]
- The periodicity of stocktakes and spot checks differs according to the manual, procedure or policy. For example, the Defence Instruction (General) Logistics 4-3-014 *Stocktaking of Defence Assets*, refers to 100 per cent annual stocktakes of explosive ordnance holdings and requires fortnightly checks of explosive ordnance,[172] as does the ESCM. However the DSM refers to minimum monthly spot checks of explosive ordnance and the Navy policy document also refers to a monthly muster of explosive ordnance holdings.[173]

---

[170] In October 2010 Defence informed the ANAO that DI(G) LOG 4-3-014 *Stocktaking of Defence Assets*, issued 29 June 2005 is considered by Defence to be the authoritative document for stocktaking requirements.

[171] In January 2011, Defence informed the ANAO that DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* has been re-drafted and is expected to be approved and released in the first half of 2011. Defence also informed the ANAO that these terminology changes will subsequently be reflected in other policy and procedural documents throughout Defence although, unless deemed critical, this may not occur until the next scheduled revision of the appropriate policy or procedure.

[172] DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* refers to SECMAN 4 for this requirement. SECMAN 4 was cancelled in the early 2000s and replaced with the *Defence Security Manual*. The reference to SECMAN 4 is therefore a reference to a document that was not current at the time of the audit. In January 2011, Defence informed the ANAO that the upcoming update to DI (G) will update this reference.

[173] In January 2011, Defence informed the ANAO that the ESCM was amended in December 2010 to align the minimum periodicity requirement for spot checks of explosive ordnance with the requirements in the DSM.

4.43 In January 2011, Defence informed the ANAO that DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* has been re-drafted and is expected to be promulgated in the first half of 2011. Additionally Defence informed the ANAO that the revised policy clearly defines the following terminology:

- A Stocktake of all Defence assets (less Land, Building, Infrastructure and Other Plant and Equipment) is to be conducted once every two years. The stocktake may be conducted progressively or at one time. This will include Explosive Ordnance. A Group or Service (e.g. Capability Manager or in the case of EO, Defence Security Agency) may elect to direct additional 'counts' that should be referred to as 'Assurance Checks'. This may include Explosive Ordnance.
- Assurance Checks are conducted to provide (Defence) Management with verifiable proof that consistent governance procedures are applied to the management of assets for which Defence is responsible. The term will 'replace' for example musters, census, % [percentage] check of holdings and spot checks.

The definitions (clarification) of the two terms is new to Defence and it will take a little time to be promulgated (and accepted). The review of the DI(G) LOG 4-3-014 Stocktaking of Defence Assets included alignment of the 'Defence' (strategic) level policy(s) to ensure 'count frequency' however, may still include additional 'counts'.

Findings from ANAO fieldwork at Service units

4.44 The boxed text below summarises the ANAO's findings in relation to stocktaking of explosive ordnance identified during fieldwork at a sample of ADF units.

As part of the audit fieldwork conducted at a sample of ADF units from each of the Services, the ANAO interviewed unit personnel about the stocktaking of explosive ordnance, including how often these stocktakes were undertaken, by whom, and where the results of the stocktakes were recorded. While the majority of units visited by the ANAO were complying with Service-specific policies, the ANAO noted some instances at units where practice conflicted with written policy. These examples are listed below:

- **Records of stocktakes** – some units did not record the results of their stocktakes. One unit recorded the results of the stocktakes but did not report the results to a third party.[174]

[174] DI(G) LOG 4-3-014 *Stocktaking of Defence Assets* requires Group and DMO Division Heads 'to monitor stocktake and spot-check results for all Asset Holding Entities under their control and ensure the reporting of those results to CJLOG on a quarterly basis'.

- **Periodicity of stocktakes** – one unit visited did not undertake stocktakes regularly and informed the ANAO that this was because of staffing restrictions.
- **Independence of stocktakes** – in two cases, the individual responsible for accounting for explosive ordnance at the unit level was also undertaking the stocktakes, despite the Defence Instruction (General) Logistics 4-3-014 *Stocktaking of Defence Assets* noting that the 'personnel independent of daily warehousing/stock management and custodial functions should conduct spot-checks'[175].

Inventory Management Systems used by the Services

4.45 The sections below outline the use of inventory management systems at the unit level within Army, Air Force and Navy.

Army

4.46 Until July 2010, SDSS was the mandated system for Army units to account for explosive ordnance.[176] In addition to SDSS, some Army units use a manual paper-based system to manage their explosive ordnance transactions and holdings.

4.47 Army informed the ANAO that COMSARM is not used by Army at the unit level for the following reasons:

- Army units do not generally have access to the Defence Secret Network on which COMSARM is hosted;
- the difficulties Army sees in having personnel appropriately trained in the use of the system; and
- Army units, due to the nature of the explosive ordnance they use and hold, do not consider explosive ordnance to be a capability that needs to be classified at a level above the national security classification of 'Restricted'.

4.48 As illustrated in Figure 4.1, once an item of explosive ordnance is issued from an EO Services Contractor-managed explosive ordnance depot to an Army unit, it is marked as 'expended' or consumed in COMSARM. The

[175] Defence informed the ANAO that a spot check in this context is a random selection of locations chosen to assist in verifying the accuracy of system records. While spot checks can be conducted via both "register to floor" and "floor to register" processes, as the requirement is to check a certain percentage of NIINs, the "register to floor" method is generally used as the major means of conducting spot checks.

[176] From July 2010 MILIS has been the mandated system for Army units to manage explosive ordnance.

exception to this relates to the 15 items included on the 'COMSARM exception listing' for Army, including the M72 light anti-armour weapon (M72). There are special rules in the ESCM for accounting for M72s. Defence informed the ANAO in November 2010 that there are no special rules for accounting for the remaining 14 items on the COMSARM exception listing for Army.

Air Force

4.49 At the time of audit fieldwork, Air Force units used COMSARM, SDSS and a variety of manual systems, such as paper-based card systems to record unit holdings of explosive ordnance. At this time, COMSARM and SDSS were the two 'authorised inventory management and accounting systems' though neither were mandated.[177] COMSARM is the 'preferred' system to manage specified high cost or sensitive items. Explosive ordnance that Defence considers to be 'low value and less sensitive' are considered to be consumed or expensed once issued to Air Force units from COMSARM.[178] The majority of explosive ordnance used by Air Force is classified by Air Force at the national security classification of 'Confidential' or above.

4.50 For the high cost or sensitive items recorded in COMSARM, the ANAO was informed that Air Force units are required to report consumption to COMSARM operators to ensure the consumed explosive ordnance is removed from COMSARM and does not inflate the explosive ordnance inventory records. This requirement is not documented and explosive ordnance consumption is not reported to COMSARM operators regularly or accurately with the result being that explosive ordnance inventory balances in COMSARM for Air Force units may be incorrect.

4.51 Prior to July 2010, COMSARM was one of two 'authorised inventory management and accounting systems' used by Air Force and is the 'preferred system for EO management for the Air Force as it meets security classification requirements'.[179] However, in practice, Air Force units do not generally use COMSARM to account for explosive ordnance at the unit level. This is because,

---

[177] Department of Defence, Australian Air Publication (AAP) 3030.002, 2006, *Air Force Supply Manua*l, Section 7, Chapter 1, paragraph 12 and 13.

[178] Except where the unit is a 'non auto-consuming' unit in COMSARM – where this is the case, none of the explosive ordnance issued to that unit is expensed. There are 19 'non auto-consuming' Air Force units. Paragraphs 4.17 to 4.21 and Table 4.2 provide further detail on 'non auto-consuming' units.

[179] Department of Defence, Australian Air Publication (AAP) 3030.002, 2006, *Air Force Supply Manua*l, Section 7, Chapter 1, paragraph 12 and 13.

apart from two Air Force bases where COMSARM has been recently implemented, as discussed in 4.14 to 4.16, Air Force units do not have access to COMSARM.

4.52 Prior to July 2010, SDSS was the other 'authorised inventory management and accounting system'[180] for Air Force units and was used to account for explosive ordnance classified at or below the national security classification of 'Restricted'.[181] Since July 2010, when MILIS replaced SDSS, MILIS is the preferred system for Air Force units to manage their explosive ordnance not managed on COMSARM after being issued.

4.53 In February 2011, Defence informed the ANAO that:

- Air Force units are currently managing their EO on separate inventory and management accounting systems. The Air Force Supplement to the revised ESCM details the systems that can be used, and whilst it identifies COMSARM and MILIS as the preferred systems to be used, it does not mandate their use.
- until such time as a single Defence inventory management and accounting system is implemented, Air Force will pursue a solution based on COMSARM to account for all explosive ordnance managed by Air Force units. Air Force intends to introduce COMSARM to all Air Force units by the end of 2011.

Navy

4.54 As indicated in Table 4.1, Navy have a classified Microsoft Access® database, known as the Explosives Custodian Officer Management System (ECOMS), available to Navy ships to account for explosive ordnance. However, the system is not mandated by Navy and during this audit the ANAO found that it was not used by most Navy units due to a lack of functionality and ongoing support for the system.[182] Instead, a majority of Navy units use either computer-based spreadsheets, paper-based systems, or a

[180] Department of Defence, Australian Air Publication (AAP) 3030.002, 2006, *Air Force Supply Manua*l, Section 7, Chapter 1, paragraph 12.

[181] Department of Defence, Australian Air Publication (AAP) 3030.002, 2006, *Air Force Supply Manua*l, Section 7, Chapter 1, paragraph 13.

[182] In June 2010, Navy informed the ANAO that from 10 responses received to a Navy initiated survey on the use of ECOMS by Navy ships, eight did not use ECOMS. The ANAO notes that of the two that were listed as using ECOMS, one informed the ANAO during fieldwork that they did not use it.

combination of both to account for explosive ordnance transactions and holdings. Some Navy units also have read-only access to COMSARM.

4.55 While Navy units do not have direct access to COMSARM, all Navy explosive ordnance is accounted for in COMSARM through a manual process whereby Navy units report via signal all explosive ordnance transactions to a COMSARM operator based at Defence Establishment Orchard Hills (DEOH) who manually inputs the relevant transactions into COMSARM.

4.56 In January 2011, Defence informed the ANAO that Navy is currently investigating two potential COMSARM based initiatives to find a common and seamless accounting system to replace the use of ECOMS and locally produced spreadsheet tools on board Navy units. The first initiative involves trialling COMSARM at sea via the Defence Secret Network, currently available to Major Fleet Units. The second initiative involves the development of a limited functionality version of COMSARM with a simplified front end, which can be hosted on a ship via the Defence Restricted Network or an appropriate laptop.

Loss of visibility of explosive ordnance at the unit level

4.57 Throughout the course of the audit, the following aspects of inventory management of explosive ordnance at the unit level in the Services were identified:

- there are a range of inventory management systems that have been or are available at the unit level including COMSARM, SDSS prior to July 2010, MILIS since July 2010, computer-based spreadsheets and paper-based systems;
- the use of these inventory management systems varies by Service, and also by unit within each of the Services;
- some units use a combination of inventory management systems to manage explosive ordnance. For example, some units use a combination of stock cards, paper-based files and computer-based spreadsheets. This duplicates workload and also increases the risk of accounting errors;
- there was no reconciliation of items issued from COMSARM and receipted onto SDSS or other inventory management systems; and
- Defence loses central visibility of, what it describes as, 'low value and less sensitive' items once they are issued from its explosive ordnance depots to ADF units. This is because these items are issued off

COMSARM when issued to ADF units and if these items are not recorded in Defence's general inventory management system by the receiving ADF unit, they are not centrally visible to the wider explosive ordnance domain within Defence. The ANAO found that some ADF units were not recording their explosive ordnance holdings on the general inventory management system, instead managing these items on other inventory management systems such as computer based spreadsheets and manual stock recording systems. Defence's preliminary estimate is that, at any given point in time, ADF units collectively hold no more than $20 million of explosive ordnance on systems outside of COMSARM.

Recommendation No.3

4.58 The ANAO recommends that Defence develop an integrated inventory management system to account for explosive ordnance at the unit level.

Defence response

4.59 Defence agreed to the recommendation.

5. Security and Security Incident Management for Explosive Ordnance at Units

This chapter outlines Defence's framework for explosive ordnance security and security incident reporting and investigation and discusses some explosive ordnance incident management issues from unit visits. It also discusses Defence's information management systems and data for explosive ordnance security incidents and describes some key internal reviews of explosive ordnance security within Defence.

Introduction

5.1 Defence seeks to 'protect its people, information, assets and infrastructure from sources of harm that could weaken, compromise or destroy them' through a 'protective security regime consisting of a combination of physical, personnel, information, and information and communications technology (ICT) security measures'.[183]

5.2 The key policy documents for security management in Defence are the *Australian Government Protective Security Manual* (PSM),[184] the *Australian Government Information and Communications Technology Security Manual* (ISM)[185] and the *Defence Security Manual* (DSM).[186] These manuals 'describe the protective security policies, principles, standards and procedures to be followed by Defence personnel and by external service providers under contract'.[187]

---

[183] Department of Defence, *Defence Security Manual*, 2009, Protective Security Policy and Governance, Introduction, paragraphs 1 and 2.

[184] Commonwealth of Australia, *Australian Government Protective Security Manual*, October 2007. In June 2010, the Australian Government Protective Security Manual was replaced by the 'Protective Security Policy Framework' (PSPF) which requires the review of all current protective security policies, procedures and guidelines. The redrafting, approval, dissemination and incorporation of this work is expected to be completed by the end of 2011. All Parts of the current PSM remain in force until they are replaced by new policies, protocols and guidelines under the PSPF. Source: Attorney General's Department website.

[185] Commonwealth of Australia, *Australian Government Information and Communications Technology Security Manual*, September 2009.

[186] Department of Defence, *Defence Security Manual*, 2009. This was the current version of this manual at the time of fieldwork for this audit.

[187] Department of Defence, *Defence Security Manual*, 2009, Protective Security Policy and Governance, Introduction, paragraph 2.

5.3 A revised version of the DSM was released in August 2009[188] in response to a number of recommendations made in the 2007 WME Audit. The August 2009 version of the DSM incorporated changes that included:

- aligning security incident requirements related to explosive ordnance with the requirements in other key Defence policy documents such as the Chief Executive's Instructions[189] and the then DI(G)ADMIN 45-2 *Reporting and Investigation of Alleged Offences within the Australian Defence Organisation;*[190]
- consolidating security policy for explosive ordnance into one section of the manual[191] rather than having it dispersed throughout the manual; and
- prohibiting all unaccompanied access to any licensed explosive ordnance facility.[192] This is discussed further in paragraphs 5.28 to 5.30.

Defence's requirements for managing explosive ordnance security incidents

5.4 Defence's DSM states:

> Defence's ability to detect, assess and mitigate security vulnerabilities is dependant upon accurate, timely and consistent reporting of all security

---

188 With full compliance by 7 October 2009 per Defence's 'Transition from DSM Edition 2 to the DSM':

> Defence will transition to full compliance with the electronic *Defence Security Manual* by 7 October 2009, which will be marked by the reissue of Defence Instruction (General) (DI(G) ADMIN 20–29 *Defence Security Manual*. In November 2010, Defence informed the ANAO that this DI(G) was reissued in May 2010.

Source: '*Defence Security Manual* (DSM) Edition 2 Transition from DSM Edition 2 to the DSM'.

189 The Chief Executive's Instructions were updated and released in July 2009.

190 Defence Instruction (General) ADMIN 45-2 was amended and rereleased on 26 March 2010. The amendment incorporated a name change. The instruction is now known as Defence Instruction (General) ADMIN 45-2 *The reporting and management of notifiable incidents*.

191 The revised version of the DSM released in August 2009 now includes a chapter dealing specifically with the security of explosive ordnance: Chapter 67 'Explosive Ordnance Security'.

192 The DSM defines a licensed explosive ordnance facility as:

> The generic designation of any building, site or area at which explosive ordnance (EO) is or is intended to be stored, packaged or unpackaged, prepared, inspected, maintained, loaded or unloaded to aircraft or vehicles of all types, e.g. all danger buildings such as explosives storehouses, igloos, laboratories, ready use compartments, EO preparation areas or buildings, EO loading aprons, EO preload areas, air movements explosive ordnance aprons, aircraft safety points and aircraft hardened shelters as authorised by the Licensing Authority.
>
> Source: Department of Defence, *Defence Security Manual*, 2009, Glossary.

incidents across Defence. Information collected assists in the formulation of policy, supports security decision making, identifies training deficiencies and helps to establish security review priorities. Comprehensive, rigorous and lawful investigations can form the basis of administrative actions and criminal proceedings, and can act as a deterrent to illegal activities.[193]

5.5 To effectively manage explosive ordnance security incidents, Defence's documented requirements for managing these incidents must provide Defence personnel with clear direction to enable them to:

- correctly identify an explosive ordnance security incident; and
- report that incident in accordance with Defence requirements.

Identifying an explosive ordnance security incident or notifiable incident

5.6 Defence's ability to adequately protect explosive ordnance through effectively detecting, assessing and mitigating security vulnerabilities, requires Defence personnel to be able to easily identify an explosive ordnance security incident. During the fieldwork for this audit, the ANAO found that, despite the revisions to key Defence policies and procedures related to explosive ordnance security as a result of recommendations made in the 2007 WME Audit, these policies and procedures still contain confusing layers of definitions in different documents and within different parts of the same document. This is discussed further in paragraphs 5.7 to 5.12.

Definition of an explosive ordnance security incident

5.7 The ANAO notes that Defence's definitions in the DSM as they relate to explosive ordnance differ from those in the PSM and within the DSM itself. Specifically:

- the definitions of a 'major security incident', as it relates to explosive ordnance, differ between the PSM and the DSM; and
- the definitions of a 'major security incident', as it relates to explosive ordnance, differ between the glossary of the DSM and those in Chapter 67 'Explosive Ordnance Security' and Chapter 12 'Security Incidents and Investigations', of the DSM.

[193] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 16, Security Incidents and Investigations, p. 1, paragraph 12-1.

DSM definition for a notifiable incident involving explosive ordnance

5.8 Chapter 67 'Explosive Ordnance Security', also defines 'notifiable incidents involving EO [explosive ordnance]' as including, but not limited to, any:

a) loss, theft, attempted theft or discovery [of explosive ordnance];

b) actual or attempted break ins to licensed EO facilities; and

c) loss, compromise or theft of any keys, cards or other access devices associated with EO security and storage.[194]

Defence Instruction (General) ADMIN 45-2 'The reporting and management of notifiable incidents' definition for a notifiable incident involving explosive ordnance

5.9 Defence released a complete revision of the DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents*[195] on 26 March 2010. This Defence Instruction articulates the mandatory requirements for reporting and managing notifiable incidents in Defence.

5.10 The definition of a notifiable incident in this Defence Instruction includes any incident that:

> is a suspected security incident, (excluding 'minor security incidents'[196]), defined in annex A whether intentional, negligent or accidental, or results from a failure to comply with a security requirement outlined in the *electronic Defence Security Manual* (DSM), Defence Security Authority (DSA).[197]

5.11 Annex A of this Defence Instruction then defines a security incident as including the:

> loss or theft of weapons, associated equipment (weapon parts, combat body armour, night fighting equipment and night vision equipment) and explosive

---

194 Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, paragraph 67.61.

195 DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents*, 26 March 2010. DI(G) ADMIN 45-2 was amended and rereleased on 26 March 2010. The amendment incorporated a name change. The instruction is now known as DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents*.

196 Minor security incidents are defined in this Defence Instruction in Annex A, paragraph 1(p) by reference to the definition of 'minor security incidents' in the *Defence Security Manual* which defines 'minor security incidents' as security incidents that are not 'major security incidents'. Source: *Defence Security Manual*, 2009, Part 2 and Chapter 12.

197 Defence Instruction (General) ADMIN 45-2 *The reporting and management of notifiable incidents*, 26 March 2010, paragraph 6(d).

ordnance (explosive ordnance includes all ammunition, propellants, pyrotechnics and explosives);[198] or

inappropriate handling and storage of classified information, weapons, associated equipment and explosive ordnance;.[199]

5.12 The relationship between a notifiable incident and a major security incident as they relate to explosive ordnance is not clear from the documented Defence definitions. The ANAO sought clarification from Defence on the difference between what Defence considers to be an explosive ordnance security incident categorised as a 'major security incident' and one categorised as a 'notifiable incident'. In November 2010, Defence informed the ANAO that there should be no difference, suggesting there would be benefit in the adoption of a common terminology. In January 2011, Defence informed the ANAO that the confusing layers have been largely addressed through the issue of amendments to the DSM in December 2010.

Defence reporting requirements for explosive ordnance security incidents or notifiable incidents involving explosive ordnance

5.13 As noted in paragraph 5.6, Defence's ability to adequately protect explosive ordnance through effectively detecting, assessing and mitigating security vulnerabilities, requires Defence personnel to be able to easily identify an explosive ordnance security incident. As discussed in paragraphs 5.6 to 5.12, there is some room for improving the clarity of Defence's definitions related to explosive ordnance security incidents.

5.14 Once an explosive ordnance security incident has been identified, there must be clear, documented requirements for Defence personnel to follow in terms of reporting the incident to the correct authorities. The ANAO found that, despite the revisions to key Defence policies and procedures related to explosive ordnance security as a result of recommendations made in the 2007 WME Audit, these policies and procedures still contain confusing requirements related to reporting explosive ordnance security incidents. These are discussed further in paragraphs 5.15 to 5.24.

[198] Defence Instruction (General) ADMIN 45-2 *The reporting and management of notifiable incidents*, 26 March 2010, Annex A, paragraph (r 2.).

[199] ibid., Annex A, paragraph (r 5.).

DSM reporting requirements for security incidents involving explosive ordnance

5.15 Chapter 67 'Explosive Ordnance Security', of the DSM defines 'any actual or suspected loss, theft, or discovery of EO [explosive ordnance]'[200] as a 'major security incident'[201] and sets out the mandatory[202] reporting requirements for these types of incidents.

5.16 This chapter of the DSM also refers the reader to Chapter 12 'Security Incidents and Investigations'[203] of the DSM for further information on major security incidents but does not specify the action to be taken in the case of a 'notifiable incident'.[204]

5.17 Chapter 12 of the DSM sets out the mandatory reporting requirements for major security incidents and security related incidents involving weapons and explosive ordnance, and refers the reader to Defence Instruction (General) ADMIN 45-2 'The reporting and management of notifiable incidents'. This chapter of the DSM does not define a 'notifiable incident' nor does it specify the action to be taken in the case of a 'notifiable incident'.

5.18 Major security incidents **must**[205] be reported to the SIC [Security Incident Centre] and **must** be handled in accordance with Defence Instruction (General) ADMIN 45-2.[206]

---

200 Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, Explosive Ordnance Security, paragraph 67.60.

201 Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, Explosive Ordnance Security, paragraph 67.60. As noted in paragraph 5.7, this definition differs from that in the PSM and that in the Glossary of the DSM.

202 In the context of the requirements of this chapter of the *Defence Security Manual*, the use of the term '**must'** means 'a mandatory compliance requirement, unless the Chief Security Officer (CSO) or relevant Group Head or Service Chief or an appointed delegate has granted a dispensation'. Source: Department of Defence, *Defence Security Manual*, 2009, Part 2 and Chapter 67.12, Explosive Ordnance Security, paragraph 67.4(c).

203 The stated purpose of Chapter 12 of the DSM is 'to detail security policy for the reporting and investigation of security incidents within Defence'. Source: Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 12, Security Incidents and Investigations, paragraph 12.2.

204 Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, Explosive Ordnance Security, paragraph 67.62.

205 In the context of the requirements of this chapter of the *Defence Security Manual*, the use of the term ***must*** means 'a mandatory compliance requirement, unless the Chief Security Officer (CSO) or relevant Group Head or Service Chief or an appointed delegate has granted a dispensation'. Source: Department of Defence, *Defence Security Manual*, 2009, Part 2 and Chapter 12, Security Incidents and Investigations, paragraph 12.3(c).

5.19 This chapter of the DSM also lists special reporting requirements for security related incidents involving weapons and explosive ordnance:

> On discovering the loss, theft, or discovery of weapons, explosive ordnance or associated equipment the person in charge **must**:
>
> a. immediately report the matter to the relevant Group Head or Service Chief through the appropriate authority;
>
> b. notify the local civilian police; and
>
> c. report the incident to the SIC immediately. An information copy of the report to the Group Head or Service Chief **must** also be supplied to the CSO.[207]

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

5.20 For a notifiable incident fitting the definition in paragraph 5.10 and 5.11, that is, a security incident involving explosive ordnance, this Defence Instruction requires that the incident be reported to DSA using the form 'XP 188 Security Incident Report'.[208] It also requires the incident to be reported for information to:

- Australian Defence Force Investigative Service (ADFIS) (if suspected *Defence Force Discipline Act 1982* offence);
- Chain of Command/line management; and
- Relevant Provost Marshall (PM)[209] (PM-Navy, PM-Army or PM-Air Force).

5.21 At the time of the fieldwork for this audit, the reporting requirements for notifiable incidents under this Defence Instruction, as they relate to explosive ordnance security incidents were not consistent with those

---

[206] Department of Defence, *Defence Security Manual*, 2009, Part 2 and Chapter 12, Security Incidents and Investigations, paragraph 12.10. Note that this DI(G) underwent a complete revision including a rename and was reissued as DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents* on 26 March 2010.

[207] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 12, Security Incidents and Investigations, paragraph 12.39.

[208] Defence Instruction (General) ADMIN 45-2 *The reporting and management of notifiable incidents*, 26 March 2010, paragraph 15.

[209] Headed by officers of Lieutenant Colonel and equivalent rank of the Navy and Air Force appointed as Provost Marshal (PM), the three Service Police organisations: the Navy's Naval Police Coxswain (NPC) category, the Army's Royal Australian Corps of Military Police (RACMP) and the Air Force's Security Police (SECPOL) all of which derive their investigative authority from the *Defence Force Discipline Act 1982*. Source: Report of an audit of the Australian Defence Force Investigative Capability, July 2006.

requirements of the DSM noted in paragraphs 5.15 and 5.19. In January 2011, Defence informed the ANAO that this issue has been predominantly resolved through amendments to the DSM made in December 2010.

Chief Executive's Instructions and Financial Management Manual

5.22 Defence's Chief Executive's Instruction (CEI) 6.3, 'Loss and Recovery of Public Property' states that: 'Asset-Holding Entity managers, Unit Commanders, Branch Heads or equivalents must ensure that a Loss of Public Property in their or their staff's, Custody is reported, recorded and investigated'.[210] Additionally, under this CEI:

> A Loss of Public Property must be reported and investigated in accordance with FINMAN 5 – Financial Management Manual, chapter 6.3 Loss and Recovery of Public Property and where applicable DI(G) FIN 12–1 or DI(G) ADMIN 45–2.[211]

Defence's FINMAN 5 – Financial Management Manual requires all losses of weapons and explosive ordnance to be reported to Group Head and Inspector General of Defence and requires all losses of attractive and sensitive items to be investigated irrespective of value. Weapons are specifically listed as attractive and sensitive items and Defence's view is that explosive ordnance is covered by term 'classified equipment'.

5.23 The ANAO notes, however, that as discussed in Chapter 4 of this report not all explosive ordnance is considered by Defence to be 'classified' and suggests that Defence consider reviewing the requirements in FINMAN 5 to confirm that the relevant explosive ordnance is covered by the requirements in this document. Additionally, the reporting requirements in FINMAN 5 for losses of explosive ordnance differ from those in other authoritative Defence documents.

5.24 Table 5.1 summarises the different requirements for reporting explosive ordnance security incidents in two different chapters of the DSM, DI(G) ADMIN 45-2 and FINMAN 5.

---

[210] Department of Defence, 25 September 2009, Chief Executive's Instruction (CEI) 6.3, 'Loss and Recovery of Public Property' paragraph 6.3.1.3.

[211] ibid., paragraph 6.3.1.4.

Table 5.1

Requirements for reporting of explosive ordnance related security incidents

DSM - Chapter 67 Explosive Ordnance	DSM - Chapter 12 Security Incidents and Investigations	DI(G) ADMIN 45-2 The reporting and management of notifiable incidents	FINMAN 5
the person in charge must: a) immediately report the matter to the appropriate authority in their Group or Service; b) notify the local state or territory police, and c) report the incident to the DSA Security Incident Centre (DSA SIC) within 24 hours.[212]	the person in charge must: a) immediately report the matter to the relevant Group Head or Service Chief through the appropriate authority; b) notify the local civilian police; and c) report the incident to the SIC immediately. An information copy of the report to the Group Head or Service Chief must also be supplied to the CSO [Chief Security Officer].[213]	<u>for action:</u> DSA (Refer Form XP 188-Security Incident Report, available on the Defence Web Forms System or in the DSM). <u>for information:</u> ADFIS [Australian Defence Force Investigative Service] (if suspected DFDA [*Defence Force Discipline Act 1982*] offence). Chain of Command/line management. Relevant PM (PM-N, PM-A or PM-AF).[214]	All losses of weapons and explosive ordnance to be reported to Group Head and Chief Audit Executive. All losses of attractive and sensitive items to be investigated irrespective of value.

Source: ANAO from Department of Defence documentation.

Clear and concise definitions required

5.25 The confusing layers of definitions and requirements in different Defence documents and within different parts of the same document remove the clarity around the requirements for managing explosive ordnance security incidents and could limit the effectiveness of Defence's policy and procedures for managing explosive ordnance security incidents. In January 2011, Defence informed the ANAO that the definitions and requirements within some key

[212] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, Explosive Ordnance Security, paragraph 67.60.

[213] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 12, Security Incidents and Investigations, paragraph 12.39.

[214] Defence Instruction (General) ADMIN 45-2 *The reporting and management of notifiable incidents*, 26 March 2010, paragraphs 14 (Table of Notifiable Incidents – Item 4 and 15).

Defence documents has been addressed to some extent through amendments to the DSM made in December 2010.

Recommendation No.4

5.26 The ANAO recommends that Defence take steps to remove the inconsistencies in the definitions and requirements for the management of explosive ordnance security incidents in Defence policy and procedural documents.

Defence response

5.27 Defence agreed to the recommendation.

Defence ban on unaccompanied access to explosive ordnance

5.28 As discussed in paragraph 1.14, the theft of military rocket launchers by an ADF member led to the 2007 WME Audit. In September 2008, in response to a recommendation in the 2007 WME Audit, the CDF issued a directive prohibiting unaccompanied access to any Defence licensed explosive ordnance facilities.

5.29 The revised version of the DSM released in August 2009 incorporated a change prohibiting unaccompanied access to explosive ordnance facilities:

> Theft by a trusted insider represents a significant security risk. For this reason, apart from EO [explosive ordnance] laboratories, unaccompanied access to licensed EO facilities **must not**[215] occur under any circumstances. Unaccompanied access to EO in laboratories **must**[216] be risk managed.[217]

[215] In the context of the requirements of this chapter of the *Defence Security Manual*, the use of the term '**must'** and '**must not'** means 'a mandatory compliance requirement, unless the Chief Security Officer (CSO) or relevant Group Head or Service Chief or an appointed delegate has granted a dispensation'. Source: Department of Defence, *Defence Security Manual*, 2009, Part 2 Chapter 67, Explosive Ordnance Security, paragraph 67.4(c).

[216] In the context of the requirements of this chapter of the *Defence Security Manual*, the use of the term **must** and **must not** means 'a mandatory compliance requirement, unless the Chief Security Officer (CSO) or relevant Group Head or Service Chief or an appointed delegate has granted a dispensation'. Source: Department of Defence, *Defence Security Manual*, 2009, Part 2 Chapter 67, Explosive Ordnance Security, paragraph 67.4(c).

[217] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, Explosive Ordnance Security, paragraph 67.42.

An authorised individual, who is named in the Security Registry, **must**[218] be present at all times when EO is accessed from a licensed EO facility.[219]

5.30 The boxed text below summarises the issues related to unaccompanied access to explosive ordnance identified during the ANAO's fieldwork visits to a sample of ADF units and subsequent advice received from Defence.

The requirement related to unaccompanied access to explosive ordnance holdings was well known by ADF personnel at unit level, however the requirement does create some challenges and confusion at times, for example:

- During audit fieldwork, a number of ADF units informed the ANAO that this requirement can be difficult to comply with. This was particularly the case for Navy, where the ANAO was informed that under certain states of ship readiness at sea, unaccompanied access is extremely difficult to manage and posed an unacceptable level of operational risk in certain circumstances. The ANAO sought further information on how Navy was managing its inability to comply with this mandatory requirement in the DSM. In November 2010, Defence informed the ANAO that in late October 2010, DSA and Navy agreed that this mandatory requirement contained in the DSM will not apply to Navy under certain circumstances, that this change will be documented in a revised version of the DSM and that these exceptions to the mandatory requirement will be documented in a revised version of Navy's primary document for managing explosive ordnance, Australian Book of Reference (ABR) 862 Volume 2,'Navy Technical Manual Maritime Explosive Ordnance Safety' In January 2011, Defence informed the ANAO that this issue has been predominantly resolved through an amendment to the DSM made in December 2010.
- During fieldwork visits, ANAO officers were taken to an explosive ordnance facility that were already open and only one Defence staff member was in attendance when the audit team arrived. On other occasions, ANAO officers were present when a number of explosive ordnance facilities were opened for the ANAO visit with only one Defence staff member present.
- The ANAO noted during fieldwork that there is some confusion over the requirements for the management of keys to explosive ordnance facilities. The requirements for managing keys to explosive ordnance facilities are not documented in Chapter 67, Explosive Ordnance Security but in an annex to the DSM chapter on physical security.[220] The ANAO observed varying degrees of security for keys to explosive ordnance storage facilities at units, from these keys being locked in biometric key lockers to keys stored in lockable containers that were left unlocked at the time of the ANAO audit visit.

[218] In the context of the requirements of this chapter of the *Defence Security Manual*, the use of the term **must** and **must not** means 'a mandatory compliance requirement, unless the Chief Security Officer (CSO) or relevant Group Head or Service Chief or an appointed delegate has granted a dispensation'. Source: Department of Defence, *Defence Security Manual*, 2009, Part 2 Chapter 67, Explosive Ordnance Security, paragraph 67.4(c).

[219] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 67, Explosive Ordnance Security, paragraph 67.43.

[220] Department of Defence, Defence, *Defence Security Manual*, 2009, Part 2, Chapter 60, Physical Security, Annex I.

Management of explosive ordnance security incidents

2007 WME Audit findings and recommendations

5.31 The 2007 WME Audit identified that Defence had a limited ability to monitor, track and assess the level and type of loss of WME due to the separate reporting and investigation systems used throughout Defence, and concluded that this had resulted in a 'fragmented WME incident reporting, recording and incident investigation system'.[221]

5.32 The 2007 WME Audit made a number of recommendations to enhance the role and capability of DSA in the areas of audit, review, compliance and remediation of WME security through changes to policies, procedures and systems.[222]

5.33 In late 2008, Defence announced that a directorate within the DSA, established following the 2007 WME Audit, was to conduct security performance reviews to analyse and assess the effectiveness of WME security policy, standards and practice and conduct security incident trend analysis to guide future security performance reviews.

Explosive ordnance security incident data

5.34 Explosive ordnance security incidents in Defence are managed on the Defence Policing and Security Management System (DPSMS), along with all non-explosive ordnance security incidents. The DPSMS was introduced in 2008 to partially address the issues identified in Defence's 2007 WME audit associated with the fragmented recording and investigation of security

---

[221] Department of Defence, 'Report of the Weapons, Munitions and Explosives Security Performance Audit', 17 August 2007, p. 109.

[222] Specifically, 2007 WME Audit Recommendations 18a to 18c. Recommendation 18c recommended that Defence improve systems and procedures for reporting, recording and monitoring WME security incidents and investigations with the aim of providing a single common system within Defence linked to Defence's WME accounting systems. Defence rolled this recommendation into 2007 WME Audit recommendations 2a and 2b which recommended that Defence improve the policies and systems for the management and accounting of WME to enhance visibility and control throughout their life cycle and recommended that WME accounting systems be managed to ensure automatic reporting of discrepancies in WME to the DSA Security Incident Centre. In January 2011 Defence informed the ANAO that progress reporting on the status of 2001 WME Audit recommendations 2a, 2b and 18c has been suspended until Defence completes an investigation into security and functionality issues associated with the transition to a single explosive ordnance inventory management and accounting system. Defence also informed the ANAO that while a firm date for full implementation of this 2007 WME Audit recommendation is yet to be established, it is expected that the implementation of the approved project strategy will be completed by 2016.

incidents. During this audit, the ANAO sought further information on Defence's capacity to conduct trend analysis in relation to explosive ordnance security incidents. The ANAO requested details[223] of explosive ordnance security incidents from 2004 involving the loss of explosive ordnance. Extracting this data from Defence's security incident data management systems proved to be a labour intensive task for Defence staff due to limitations in Defence's security incident management data.

5.35 The data, the systems and some of the associated limitations of both are discussed below.

Explosive ordnance security incidents reported from 2008 to May 2010

5.36 As of 10 May 2010, Defence's incident and investigation case management system, the Defence Policing and Security Management System (DPSMS Stage 2), held 22 reported security incidents involving explosive ordnance for the period 2008 to 10 May 2010.[224] Table 5.2 provides a breakdown of these 22 reported incidents by ADF entity and the status of the incident according to the data available to the DSA.

[223] The request sought the following information related to explosive ordnance security incidents: description of the explosive ordnance items involved; the ADF Service involved; how the incident was discovered; when in the explosive ordnance life cycle was it discovered; what action taken; incident outcome; current status of the incident; action taken to prevent recurrence; and the number of days between:

- when the incident occurred to when it was reported to DSA;
- when the incident was reported to when an investigation commenced; and
- when the investigation commenced to when the investigation was completed.

[224] Ten incidents in 2008, seven incidents in 2009 and five incidents in 2010 to 10 May 2010.

Table 5.2

Reported security incidents involving the loss of explosive ordnance from 2008 to 10 May 2010

ADF entity	Number of reported incidents	Number of reported incidents where items were not recovered	Number of reported incidents where items were recovered	Number of reported incidents where the outcome of any Defence investigation is not known.
Army	15	7	4	4
Air Force	1	1	0	0
Navy	4	4	0	0
JLC	2	1	1	0
Total	**22**	**13**	**5**	**4**

Source: Department of Defence

5.37 As shown in Table 5.2 Defence's DPSMS did not have a record of the outcome of four[225] of the 22 reported explosive ordnance security incidents from 2008 to 10 May 2010. Defence informed the ANAO that where the outcome of an incident is indicated as 'unknown', this is where an inquiry or investigation has been completed by the unit that where the breach occurred, however the inquiry report is not provided to DSA to identify the incident outcome or actions taken to prevent recurrence. In accordance with the DSM, units are required to provide the report of an investigation into a security incident to the DSA.[226] In January 2011, Defence informed the ANAO that is has commenced regular review of all outstanding investigation reports.

[225] All four incidents related to Army.

[226] Department of Defence, *Defence Security Manual*, 2009, Part 2, Chapter 12, Security Incidents and Investigations.

5.38 Additionally, the time that elapsed between when an incident occurred and when it was reported to a Defence Investigative Authority[227] varied from between one day (eight incidents) to 49 days (one incident). Defence informed the ANAO that this occurs because in some cases an incident may be investigated by the relevant unit itself prior to reporting to a Defence Investigative Authority (DIA).

Explosive ordnance security incidents reported from 11 May 2010 to 8 October 2010

5.39 From 11 May 2010 to 8 October 2010, during the course of this audit, a further 11 explosive ordnance security incidents were reported to the DSA of which 10 were reported by Army. In respect of these 11 incidents:

- the items were not recovered in five instances;
- the outcome of the investigation into two of the incidents was unknown to the DSA; and
- the remaining four incidents were still under investigation by Defence.

Limitations of Defence's explosive ordnance incident data and associated systems

5.40 As discussed in paragraph 5.34, the ANAO sought details from Defence of losses of explosive ordnance commencing from 2004. Defence informed the ANAO that the standard reports from Defence's incident and investigation case management system, the DPMS, could not provide all of the information requested by the ANAO. As a result, each of the explosive ordnance incidents needed to be checked individually to provide the information requested by the

[227] Defence has a number of Defence Investigative Authorities (DIA) that conduct investigations for the Department of Defence and the ADF. They are:

- Headed by a Band 2 level member of the Australian Public Service (APS), the Inspector General Division (IG-D) of the Department of Defence. IG-D investigations are conducted in accordance with a 1991 Directive and a 2005 Charter, both issued by the Secretary of the Department of Defence and the CDF.
- Headed by an Executive Level 2 APS member, the Security Investigations Unit (SIU) of the Defence Security Authority (DSA) is responsible for the conduct of complex and major security investigations. Its investigations are conducted under the authority of the Secretary of the Department of Defence and the CDF.
- Headed by officers of Lieutenant Colonel and equivalent rank of the Navy and Air Force appointed as Provost Marshal (PM), the three SP organisations: the Navy's Naval Police Coxswain (NPC) category, the Army's Royal Australian Corps of Military Police (RACMP) and the Air Force's Security Police (SECPOL) all of which derive their investigative authority from the DFDA.

Source: Department of Defence, Report of an Audit of the Australian Defence Force Investigative Capability, July 2006, paragraph 1.8, pp. 2-3.

ANAO. However, Defence also informed the ANAO that most of the information requested by ANAO can be produced from existing reports and that it is technically possible to build new DPSMS reports to report this information.

5.41 Additionally, Defence informed the ANAO that the explosive ordnance incidents and investigations recorded 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 may not be readily identifiable as an explosive ordnance related security incident from the reports.

5.42 Defence informed the ANAO that one of the major issues with WME incidents (which include explosive ordnance incidents) is that not all the incidents involving WME are being correctly identified as security incidents or being reported to DSA, and it is common for WME incidents to be recorded as 'Fraud' or 'Policing' incidents under the category of 'theft of service property' instead of a 'Security' incident which incorporates security incidents involving weapons, munitions or explosives. This means that each record in the DPSMS has to be manually scanned for anything that would indicate it is an explosive ordnance related security incident.

5.43 The following errors were found in the data provided to the ANAO by the DSA during the course of this audit:

- As noted paragraph 1.14 of this Report, in July 2010 it was reported in the media that 2572 rounds of assault rifle ammunition had gone missing during May 2007 in the Northern Territory. This explosive ordnance security incident was not included in the data provided to the ANAO during the course of this audit, because it was incorrectly classified in the DPSMS as a 'recovery' of explosive ordnance and was accidentally overlooked in the manual search of the database records for losses of explosive ordnance.
- As noted paragraph 1.14, a 20 mm round was stolen from a Defence location in the Northern Territory. This explosive ordnance security incident was not included in the data provided to the ANAO during the course of this audit, because it was recorded in Defence's DPSMS as a 'recovery'. The explosive ordnance was located during a room search by Service Police and was never reported as an item of explosive ordnance that was missing.

- An explosive ordnance security incident reported in a brief prepared by Navy for a Senate Standing Committee in October 2009 listed a number of ammunition rounds as having gone missing between January and March 2009. These incidents were not included in the data provided to the ANAO. Defence informed the ANAO that this was because the incident was reported as a 'recovery' of explosive ordnance instead of as a loss of explosive ordnance.
- As noted in paragraph 1.14, in December 2006, it was reported in the media that 10 light anti-armour weapons (M72s) were stolen from the ADF.[228] This incident is recorded in Defence's DPSMS dated 5 April 2007 and reports nine M72s missing. Defence informed the ANAO that at the time the incident was brought to the attention of Defence by the AFP in late 2006, Defence was unable to record the incident on Defence's incident management database in a way that enabled the incident to be reported as a WME incident. Defence informed the ANAO that the figure of nine is based on the fact that the individual eventually convicted of the theft of the M72s stated that he stole 10 of these items, however one of these was recovered by police—the recovery of which led to the investigation—Defence therefore have recorded nine as missing.

5.44 The data discrepancies described above indicate that Defence may not be aware of missing explosive ordnance until it is recovered.

5.45 For the majority of the explosive ordnance security incidents reported, Defence's security incident and investigation case management system did not include records of the time between when an explosive ordnance security incident was reported and when an investigation commenced, or the time

[228] ABC, 14 December 2006, *Army link to stolen weaponry*, available from <http://www.smh.com.au/news/national/army-link-to-stolen-weaponry/2006/12/14/1165685828177.html>, [accessed 15 January 2010].

Sydney Morning Herald, *Rocket launcher theft: bail denied*, 11 April 2007, available from <http://www.smh.com.au/news/national/rocket-launcher-theft-bail-denied/2007/04/11/1175971162175.html> [accessed 2 March 2010].

The Daily Telegraph, 11 December 2008, *Six rocket launchers remain missing after army theft*, available from <http://www.dailytelegraph.com.au/news/rocket-launchers-remain-missing/story-e6freuy9-1111118281946., [accessed 13 July 2010].

The Australian, 17 October 2009, *No sign of stolen rocket launchers*, available from <http://www.theaustralian.com.au/news/no-sign-of-stolen-rocket-launchers/story-e6frg6o6-1225787746734>, [accessed 13 July 2010].

between when an investigation commenced and when it was completed. The ANAO was informed that gaps in this data resulted from cases where the unit involved has conducted an inquiry prior to reporting the incident, or the incident was referred back to the relevant unit for inquiry and the incident outcomes and/or the time taken to investigate the incident are not known, as they are not reported back to the DSA. As noted in paragraph 5.37, unit are required to provide a report on the outcomes of the incident investigation to the DSA. These shortcomings in Defence's security incident management data and reporting mean it is difficult for Defence to have a complete picture of explosive ordnance security incidents. This then hinders Defence's ability to examine trends in this area and identify and manage associated risks. As noted in paragraph 5.4, Defence considers that its ability to detect, assess and mitigate security vulnerabilities is dependant upon accurate, timely and consistent reporting of all security incidents. The ANAO found that, at the time of audit fieldwork, Defence has made limited progress in achieving accurate, timely and consistent reporting of explosive ordnance incidents within Defence since the 2007 WME Audit thereby limiting Defences' ability to detect, assess and mitigate security vulnerabilities in relation to explosive ordnance. In January 2011 Defence informed the ANAO that DSA is now regularly reviewing the progress of those incidents where a report has not been provided.

5.46 As at October 2010, 16 explosive ordnance security incidents had been reported for the year to date. This is well in excess of the seven reported incidents for the whole of 2009. Defence informed the ANAO that this is in line with the trend for the number of reported security incidents as a whole and is most likely due to increased awareness of the requirement to report security incidents and the existence of the centralised DPSMS, rather than an actual increase in the number of explosive ordnance security incidents.

5.47 Defence informed the ANAO that the combination of a number of recent improvements made in the security incident reporting domain—including the increased awareness of the requirements around reporting security incidents; the March 2010 release of the revised Defence Instruction (General)[229] on reporting security incidents; the online availability of Defence's security incident reporting form; and the centralised DPSMS—has improved

[229] Defence Instruction (General) DI(G) ADMIN 45-2 *The reporting and management of notifiable incidents*, 26 March 2010.

the visibility of security incidents in Defence. Further, Defence informed the ANAO that it is likely that 2010 will be able to be used as a benchmark year from which Defence could then carry out trend analysis on security incidents.

5.48 Notwithstanding the recent changes to Defence's explosive ordnance security incident procedures and systems implemented since the 2007 WME Security Audit, the ANAO considers that, given Defence's inability to provide a complete and correct set of data on explosive ordnance losses in recent years, there continues to be significant room for improvement in Defence's management and reporting of explosive ordnance security incidents.

Security incident reporting in Defence

5.49 Defence informed the ANAO that DSA produces a number of security incident reports including:

- A weekly report of all security incidents which is provided to the Director of Security Intelligence and Investigations within the DSA. These reports are also available on DSA's internal intranet.
- Monthly reports are produced by Defence Group and Service, however Defence informed the ANAO that these reports are not circulated unless requested by the various Group Heads which is rare. Defence informed the ANAO that the three ADF Services rarely request security incident reporting data from DSA.

5.50 There is no trend analysis and reporting conducted on explosive ordnance security incidents within Defence.

Recommendation No.5

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

Defence response

5.52 Defence agreed to the recommendation.

Ian McPhee
Auditor-General

Canberra ACT
19 April 2011

Appendices

Index

A

Air Force, 11–13, 15, 18, 22, 24, 32–33, 44, 46–47, 52, 58, 61, 65, 67, 71–73, 75, 77–84, 87, 89, 92–94, 103, 110, 111
Army, 11–12, 14–15, 22, 24, 32–33, 37–38, 41, 44, 46–48, 52, 55, 58, 61, 65, 67, 73, 75, 78, 79, 81, 82, 84, 89–90, 92, 103, 110–111, 113, 122

C

Computer System for Armaments (COMSARM), 11, 13–14, 17–18, 20–23, 31, 33–37, 42–43, 45, 51, 54, 67, 68–70, 75–77, 79–87, 92–96

D

Defence Policing and Security Management System (DPSMS), 7, 108–114
Defence Security Manual (DSM), 11, 20, 29, 34, 49–50, 63–64, 89–90, 97–107, 110

E

Electronic Supply Chain Manual (ESCM), 20, 29, 49, 63–65, 68, 71, 89, 90, 93–94

M

Military Integrated Logistics Information System (MILIS), 8, 13, 16–18, 21–24, 31, 33, 35, 40, 43, 64, 65, 73, 76–79, 85–87, 92, 94–95

N

Navy, 11, 14–15, 22, 24, 31–36, 44, 46–47, 53–54, 58, 61, 65–67, 70–71, 73, 77–78, 80, 81–84, 89, 90, 92, 94–95, 103, 107, 110–111, 113

O

Orme Review, 39– 40, 43, 75

S

System of Defence Instructions (SoDI), 8, 44, 58–61, 64

W

Weapons, Munitions and Explosives (WME) Security Performance Audit 2007, 12–13, 19, 21, 23, 41–43, 48–50, 63, 75–76, 98–99, 101, 106, 108, 114

Series Titles

ANAO Audit Report No.1 2010–11
Implementation of the Family Relationship Centres Initiative
Attorney-General's Department
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.2 2010–11
Conduct by Infrastructure Australia of the First National Infrastructure Audit and Development of the Infrastructure Priority List
Infrastructure Australia

ANAO Audit Report No.3 2010–11
The Establishment, Implementation and Administration of the Strategic Projects Component of the Regional and Local Community Infrastructure Program
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.4 2010–11
National Security Hotline
Australian Security Intelligence Organisation
Attorney-General's Department
Australian Federal Police

ANAO Audit Report No.5 2010–11
Practice Incentives Program
Department of Health and Ageing
Medicare Australia

ANAO Audit Report No.6 2010–11
The Tax Office's implementation of the Client Contact - Work Management - Case Management System
Australian Taxation Office

ANAO Audit Report No.7 2010–11
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2009 Compliance)

ANAO Audit Report No.8 2010–11
Multifunctional Aboriginal Children's Services (MACS) and Crèches
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.9 2010–11
Green Loans Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency

ANAO Audit Report No.10 2010–11
Centrelink Fraud Investigations

ANAO Audit Report No.11 2010–11
Direct Source Procurement

ANAO Audit Report No.12 2010–11
Home Insulation Program
Department of the Environment, Water, Heritage and the Arts
Department of Climate Change and Energy Efficiency
Medicare Australia

ANAO Audit Report No.13 2010–11
Implementation and Administration of the Civil Aviation Safety Authority's Safety Management System Approach for Aircraft Operators

ANAO Audit Report No.14 2010–11
Capitalisation of Software
Australian Bureau of Statistics
Civil Aviation Safety Authority
IP Australia

ANAO Audit Report No.15 2010–11
Food Standards Australia New Zealand

ANAO Audit Report No.16 2010–11
Centrelink's Role in the Process of Appeal to the Social Security Appeals Tribunal and to the Administrative Appeals Tribunal
Centrelink
Department of Education, Employment and Workplace Relations
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.17 2010–11
2009–10 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.18 2010–11
Government Business Managers in Aboriginal Communities under the Northern Territory Emergency Response
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.19 2010–11
Army Aboriginal Community Assistance Program
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.20 2010–11
Administration of the Wine Equalisation Tax
Australian Taxation Office

ANAO Audit Report No.21 2010–11
Indigenous Housing Initiatives: the Fixing Houses for Better Health program
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.22 2010–11
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2010

ANAO Audit Report No.23 2010–11
Home Ownership of Indigenous Land Program
Department of Families, Housing, Community Services and Indigenous Affairs
Indigenous Business Australia

ANAO Audit Report No.24 2010–11
The Design and Administration of the Better Regions Program
Department of Regional Australia, Regional Development and Local Government

ANAO Audit Report No.25 2010–11
Administration of the Trade Training Centres in Schools Program
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.26 2010–11
Management of the Tender Process for a Replacement BasicsCard
Department of Human Services

A**NAO Audit Report No.27 2010–11**
Restoring the Balance in the Murray-Darling Basin
Department of Sustainability, Environment, Water, Population and Communities

ANAO Audit Report No.28 2010–11
Management of the Australian Broadband Guarantee Program
Department of Broadband, Communications and the Digital Economy

ANAO Audit Report No.29 2010–11
Management of the Implementation of New Policy Initiatives
Australian Federal Police

ANAO Audit Report No.30 2010–11
Digital Education Revolution Program—National Secondary Schools Computer Fund
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.31 2010–11
Administration of the Superannuation Lost Members Register
Australian Taxation Office

ANAO Audit Report No.32 2010–11
Northern Territory Night Patrols
Attorney-General's Department

ANAO Audit Report No.33 2010–11
The Protection and Security of Electronic Information Held by Australian Government Agencies

ANAO Audit Report No.34 2010–11
General Practice Education and Training
General Practice Education and Training Limited

ANAO Audit Report No.35 2010–11
Management of the Overseas Leased Estate
Department of Foreign Affairs and Trade

ANAO Audit Report No.36 2010–11
Service Delivery in CRS Australia
Department of Human Services

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office website.

Human Resource Information Management Systems	
Risks and Controls	Mar 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	Sep 2010
Implementing Better Practice Grants Administration	June 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
Preparation of Financial Statements by Public Sector Entities	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
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006

Legal Services Arrangements in Australian Government Agencies	Aug 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006