

Electronic Health Records for Defence Personnel

Department of Defence

© Commonwealth of Australia 2015

ISSN 1036-7632 (Print)

ISSN 2203-0352 (Online)

ISBN 978-1-76033-020-0 (Print)

ISBN 978-1-76033-021-7 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit

<http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <http://www.itsanhonour.gov.au/>.

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:

publications@anao.gov.au.



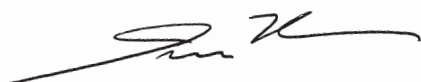
Canberra ACT
10 March 2015

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Defence titled *Electronic Health Records for Defence Personnel*. The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

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

Yours sincerely



Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

For further information contact:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7505

Fax: (02) 6203 7519

Email: publications@anao.gov.au

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

<http://www.anao.gov.au>

Audit Team

Alex Doyle
John Harper
Moustafa Abdel-Nasser
Stuart Turnbull

Contents

Abbreviations.....	7
Glossary	8
Summary and Recommendations	9
Summary	11
Introduction	11
Audit objective and scope	14
Overall conclusion.....	15
Summary of entity response	20
Recommendations	21
Audit Findings	23
1. Introduction	25
Overview of the Defence Electronic Health System	25
Related reviews and audits	32
About the audit	34
Structure of the report	37
2. Planning and Procurement	38
Introduction	38
Defining business requirements.....	38
Project scope, budget and procurement.....	41
Conclusion	52
3. System Implementation.....	55
Introduction	55
Project management and implementation	55
Security and integrity of information.....	66
Standardisation of eHealth processes	71
Conclusion	75
Appendices	79
Appendix 1: Entity Response	81
Appendix 2: Summary assessment of Defence’s overall effectiveness in delivering the eHealth system—status in 2014–15	82
Appendix 3: Business scenarios used to assess the functionality of DeHS.....	83
Index.....	86
Series Titles.....	88
Better Practice Guides	92

Tables

Table S.1:	DeHS funding approvals and basis of costings.....	13
Table 1.1:	DeHS funding approvals and basis of costings.....	28
Table 1.2:	DeHS anticipated benefits	30
Table 1.3:	Grading scheme for assessing effectiveness.....	35
Table 1.4:	Assessment of effectiveness against criteria	36
Table 2.1:	Summary assessment of Defence's effectiveness in defining DeHS business requirements.....	39
Table 2.2:	Summary assessment of Defence's effectiveness in scoping, budgeting for and procuring DeHS	42
Table 3.1:	Summary assessment of Defence's effectiveness in project managing and implementing DeHS.....	56
Table 3.2:	Summary assessment of Defence's effectiveness in protecting the security and integrity of information maintained in DeHS	67
Table 3.3:	Summary assessment of Defence's effectiveness in delivering standardised DeHS business processes.....	72
Table A.1:	Business scenarios used to assess the functionality of DeHS in supporting clinical care, practice management and reporting.....	83

Figures

Figure 2.1:	DeHS project funding approvals.....	45
Figure 2.2:	Typical steps for accessing eHealth records from the primary data centre and developing reports	50

Abbreviations

ADF	Australian Defence Force
AGD	Attorney–General’s Department
CSC	CSC Australia Pty Ltd
CDF	Chief of the Defence Force
DeHS	Defence eHealth System <i>previously Joint eHealth Data and Information System (JeHDI)</i>
eHealth	Electronic Health
EMIS	Egton Medical Information Systems
ICT	Information and Communications Technology
ISM	Australian Government Information Security Manual
JHC	Joint Health Command
MoD	UK’s Ministry of Defence
NEHTA	National eHealth Transition Authority
RPDE	Rapid Prototyping, Development and Evaluation
PCS	Primary Care System
PCEHR	Personally Controlled Electronic Health Record
PSPF	Australian Government Protective Security Policy Framework
WHS	Work health and safety <i>previously occupational health and safety (OH&S)</i>

Glossary

Defect	A problem which, if not corrected, could cause an application or ICT system to either fail or to produce incorrect results.
Health groups	The ADF refers to clinicians, dentists, nurses and other allied health providers as members of craft groups. These groups are referred to as health groups throughout this audit report.
ICT system (or IT system)	A related set of hardware and software used for the processing, storage or communication of information, and the governance framework in which it operates.
IT general controls	Policies and procedures developed to deal with identified ICT system risks, including controls over ICT governance, ICT infrastructure, security and access to operating systems and databases, and program change procedures.
Joint Health Command	A group within the Department of Defence that provides health care and contributes to the preparedness of ADF personnel for operations. JHC also develops strategic health policy and provides strategic level health advice.
Logical access controls	ICT measures used to control access to ICT systems and their information—including user identifications and authenticators such as passwords.

Summary and Recommendations

Summary

Introduction

1. The Department of Defence (Defence) provides health care services to some 80 000 Australian Defence Force (ADF) personnel throughout their service, from their induction until their discharge. ADF personnel move regularly during their military service, for postings and deployments, and they receive health care services through both military and civilian channels. The number of serving personnel, their multiple locations, mobility, and access to different channels for health care increase the complexity of maintaining complete, accurate and up to date medical records. An effective electronic health (eHealth) system assists in maintaining medical records, delivering integrated health care, and in providing valuable information to stakeholders on health care services and the health of personnel.
2. In May 2009, Defence finalised a business case to deliver a contemporary health records management system for ADF personnel. The proposed system was originally called the Joint eHealth Data and Information System (JeHDI) and was later known as the Defence eHealth System (DeHS).¹ The business case noted that the proposed system would centralise, electronically capture and manage ADF health records, and seamlessly link health data for ADF personnel. The system was also to be used to help assess the preparedness of ADF personnel for operations, and inform health groups² preparing for deployment in support of operations.
3. In February 2010, Defence approached the market seeking tenders for a proven eHealth system to meet its business requirements. CSC Australia Pty Ltd (CSC)³ was awarded the contract to implement an off-the-shelf product sourced from Egton Medical Information Systems, a United Kingdom (UK)

1 The project is referred to as DeHS throughout this audit report to be inclusive of both the business solution and the enabling ICT system.

2 The ADF refers to clinicians, dentists, nurses and other allied health providers as members of craft groups. These groups are referred to as health groups throughout this audit report.

3 Defence awarded a contract to CSC Australia Pty Ltd (CSC) to build, host and support Defence's eHealth System through to 2019–20 at a value of \$68.9 million; and awarded a \$6.1 million contract for project management services to IT services provider Oakton.

firm. The product was known as the Primary Care System (EMIS PCS)—an eHealth system used by the UK Ministry of Defence (MoD).⁴

4. The DeHS project has been managed by Defence's Joint Health Command (JHC)⁵, with the system designed, built, hosted and supported by CSC. By December 2014, DeHS was deployed and in use across Defence's Garrison Health environments. Deployment of DeHS for use in operational environments, such as on board ships, remained a planned activity.

DeHS funding approvals and basis

5. The Chief of the Defence Force (CDF) and Secretary of Defence approved acquisition and sustainment funding of \$23.3 million in June 2009 to develop DeHS in a staged approach: from prototype to pilot, and on to a mature production system by December 2011. There was an expectation at the time that the system would be hosted and managed internally as part of the Defence ICT environment, which meant that the resources applied to support Defence's extant eHealth systems could eventually be used to support the new system.

6. Since 2009 there have been two major increases to the original DeHS acquisition and sustainment budget of \$23.3 million, resulting from changes to project scope:

- In November 2010, the Minister for Defence sought concurrence from the Finance Minister for approval of the DeHS project, including significantly higher project costs.⁶ The Finance Minister agreed to the commencement of final contract negotiations with CSC, conditional on the then Department of Finance and Deregulation (Finance) agreeing to final project costs prior to Defence signing the contract. In January 2011, Finance agreed to total project costs of \$85.9 million, comprising \$54.6 million for acquisition costs and \$31.3 million for sustainment costs from 2010–11 to 2019–20.

4 In May 2006, the military version of EMIS PCS was selected by MoD as part of the Defence Medical Information Capability Programme (DMICP). The system has been implemented and is reported to support over 16 000 consultations per day.

5 As part of the Vice Chief of Defence Force (VCDF) Group, JHC develops strategic health policy, provides strategic level health advice, commands and controls, and exercises technical and financial control of ADF health units.

6 Defence projects valued from \$20 million to \$100 million required the approval of both the Minister for Defence and Minister for Finance, and those valued at \$100 million or more required the approval of Cabinet.

- In February 2014, Defence obtained approval from the National Security Committee of Cabinet to increase the DeHS budget by a further \$47.4 million to address capability shortfalls, including for the purchase of additional software licences and to fund training requirements.
7. Over time, the approved total DeHS project cost rose to \$133.3 million, some \$110.0 million higher than the original budget. At each approval stage, the project has been funded internally using Defence's departmental budget, and Defence did not request supplementary funding from government. Nevertheless, there is an opportunity cost associated with Defence allocating significant additional funds to the project. Table S.1 provides a summary of DeHS funding approvals since 2009, and the principal reasons for the increase in costs.

Table S.1: DeHS funding approvals and basis of costings

Approval date	Acquisition (\$ million)	Sustainment (\$ million)	Total (\$ million)	Costing basis and reasons for change
June 2009	20.5	2.8	23.3	a) Sustainment period to 2018–19. b) System hosted and managed internally in Defence's ICT environment. <ul style="list-style-type: none"> • <i>Not costed: deployment; re-assignment of staff from Defence's extant Health systems to support DeHS.</i>
January 2011	54.6	31.3	85.9	a) Sustainment period to 2019–20. b) System hosted and supported externally by CSC.
February 2014	84.5	48.8	133.3	a) Sustainment period to 2019–20. b) System hosted and supported externally by CSC. <ul style="list-style-type: none"> • <i>Additional funding for: software licences; training requirements; hardware, infrastructure and enhancements.</i>

Source: ANAO.

8. In summary, the principal reasons for the increase in DeHS project costs were: a one year extension of the funded sustainment period; hosting the

system externally rather than internally; and the inclusion of previously unbudgeted items such as training requirements.

9. In light of concerns about cost overruns, shortcomings in Defence's project planning and the quality of the project proposals brought forward to government, the Treasurer requested that the Auditor-General consider undertaking a performance audit of the processes used by Defence in its development of DeHS. The Auditor-General agreed to the Treasurer's request.

Audit objective and scope

10. The objective of the audit was to examine the effectiveness of Defence's planning, budgeting and implementation of an electronic health records solution for Defence personnel. The scope of this audit covered the development and implementation phases of DeHS from project inception in 2009 through to the end of 2014, and included a focus on the quality of Defence's advice to government.

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

- Defence adequately defined DeHS business requirements;
- Defence developed an appropriate DeHS project scope and budget, and adhered to government procurement policies and procedures;
- DeHS project governance and management supported effective system implementation, and the design and build of DeHS delivered intended functionality;
- DeHS has maintained the security and integrity of health information; and
- Defence established standardised eHealth processes through the use of DeHS.

Overall conclusion

12. Defence provides health care services to some 80 000 ADF personnel in many different locations using both military and civilian providers. In 2009 Defence recognised that it did not have contemporary information and patient records systems to support the delivery of ADF health services. To address this situation, Defence planned to procure a proven off-the-shelf ⁷ eHealth system to record details of health consultations, treatments and findings, and report on individual and corporate health information requirements. Procurement of the Defence eHealth System (DeHS) followed two unsuccessful earlier attempts to effectively implement an enterprise eHealth system.⁸

13. Overall, Defence's planning, budgeting and risk management for the implementation of DeHS were deficient, resulting in substantial cost increases, schedule delay and criticism within government. During the initial phases of the project, Defence did not: scope and cost key components of the project; validate project cost estimates and assumptions; obtain government approval when required; follow a project management methodology; or adequately mitigate risk by adopting fit for purpose governance and co-ordination arrangements. Defence's planning and management of the initial phases of the DeHS project were well below the standards that might be reasonably expected by Defence's senior leadership, and exposed the department to reputational damage. The initial June 2009 budget of \$23.3 million increased almost five-fold to \$133.3 million by February 2014, in response to a different ICT hosting model and a better understanding of business needs. Further, Defence initially planned to develop DeHS as a mature system by December 2011, but did not complete rollout until December 2014.

14. The DeHS project was led by Defence's Joint Health Command (JHC), which lacked experience in managing complex ICT-related projects. Further, the contribution of Defence's Chief Information Officer Group was limited; a weakness in internal project governance and coordination arrangements which introduced substantial additional risk. A routine internal audit in 2012 and a further internal audit initiated by the Commander Joint Health in 2013 identified

7 It has long been recognised that the use of off-the-shelf solutions can reduce project cost and mitigate the risk of schedule delay and cost increases in the Defence environment. See ANAO Audit Report No.6 2013–14, *Capability Development Reform*, pp. 202–3.

8 HealthKeyS and MIMI were two competing and discrete Defence eHealth systems that did not meet clinical user needs or Defence's management requirements.

major shortcomings in Defence's project management and preparedness to implement many DeHS requirements. Between 2012 and 2014, Defence strengthened project governance and management arrangements to implement both the ICT system and related business reforms. These remedial steps refocused the project and assisted the rollout of DeHS by December 2014. The system as rolled-out delivers most of the intended functionality, and notwithstanding the need for some corrective action, stakeholders have identified early benefits from the use of the system, including access to a single patient eHealth record.⁹

15. As indicated above, the ANAO identified significant weaknesses in the early stages of the project—relating to project planning and budgeting; and project management and implementation—which affected the overall project budget and timely implementation of outcomes. Following on from improvements in project management and implementation in the later stages of the project, an ongoing focus on system and business enhancements is required to realise the anticipated benefits of the system given the substantial investment made to date.

Project planning and budgeting

16. Shortcomings in project planning and budgeting were evident from the project's earliest days. Defence's initial 2009 DeHS project proposal and budget were not properly scoped, made an incorrect assumption about ICT hosting arrangements, and were not appropriately validated before approval. The approved budget did not include funding for progressive deployment of the system in the Garrison Health and operational environments, and the absence of costing detail in the proposal was not identified as a concern. Further, Defence did not seek ministerial approval of the DeHS project in 2009 in accordance with government requirements.¹⁰ Defence first informed the then Minister for Defence about the DeHS project in February 2010, before releasing the Request for Tender. In its advice, Defence informed the Minister that the

9 The Commander Joint Health informed the ANAO that while Australia-wide implementation has only recently been completed, early benefits include: improved information access and sharing between allied health professionals; more efficient administrative workflows; and improved health data analysis and reporting.

10 In April 2009, Cabinet agreed that Defence projects with a cost: of \$100 million or more required the approval of Cabinet; from \$20 million to \$100 million required the approval of both the Minister for Defence and the Minister for Finance; and below \$20 million required the approval of the Minister for Defence.

estimated cost of the project was \$19 million when the approved cost was actually \$23.3 million, and in excess of the financial threshold for approval by the Minister for Defence. The weaknesses identified by the ANAO in the project planning and advisory phase were avoidable.

17. Defence's approach to market in February 2010 differed from the DeHS business case in that it sought bids for an externally hosted system and ongoing support, rather than an internally hosted system. This change in direction had significant implications for the project's scope and budget, and contributed to a subsequent approach to government seeking approval of significantly higher project costs. Five companies responded to the tender, each with international experience in designing, building, implementing and hosting an eHealth system. The tender evaluation team assessed the tenders against the evaluation criteria and shortlisted two companies to conduct negotiations for best and final offers. This process led to the selection of CSC as the preferred tenderer on the basis that it offered a robust and proven (off-the-shelf) solution that represented value for money and reduced financial, corporate and legal risks.

18. In finalising the tender selection process in November 2010, Defence arranged for concurrent approval by the Ministers for Defence and Finance of revised DeHS project funding of \$85.9 million. A key matter raised by the Finance Minister was the conduct of an independent Gateway Review for the project.¹¹ It is not evident from Defence records why a Gateway Review was not undertaken. The subsequent history of the DeHS project indicates that the decision not to proceed with a Gateway Review was an opportunity lost.

19. Leading up to November 2013, JHC identified further impediments to delivering DeHS. Defence had not properly scoped and budgeted for system deployment and business implementation, including: changes to Defence's core ICT systems to interface with DeHS; hardware upgrades to support 1200 concurrent DeHS users; and training requirements and user software licences.¹² Defence obtained approval from the National Security Committee of Cabinet in February 2014 to increase the DeHS budget by a further \$47.4 million. In effect, Ministers were asked to support additional funding for system

11 Gateway Reviews are normally conducted for all IT projects valued at over \$10 million, and are intended to identify and focus on issues of most importance to a project, so that the project team's effort is directed to those aspects that will help the project be successful.

12 The original contract with CSC included 400 user software licences, at a cost of \$4.2 million; and in August 2014, Defence paid \$4.3 million for 600 additional licences.

components and features which should properly have been factored into the original 2009 project proposal.

Project management and implementation

20. Defence underestimated the complexity of project managing and implementing DeHS. At the outset of the DeHS project, Defence did not follow an approved program or project management methodology, even though Defence ICT projects are required to apply proven methodologies. Commencing in 2012, two internal audits, the second initiated by JHC reported major shortfalls in DeHS project management, controls, reporting and documentation. Internal audit confirmed that key assumptions underpinning the DeHS business case were not valid and without greater focus on business implementation, the project would be at risk.

21. More fundamentally, Defence underestimated the broader program and governance challenges inherent in the project, and did not mitigate key risks until mid-2012. Defence initially adopted a narrow implementation approach, focusing on delivery of the project's ICT component, rather than a broader program focus which treated DeHS as a key ICT enabler of Defence's health system and capability. In April 2012, nearly three years into the project, JHC assigned responsibility for DeHS organisational level change management to a newly formed team within JHC; and in September 2012, a program management structure was implemented to provide for joint governance oversight of ICT-related activities and business reform.

22. On a more positive note, Defence recognised the benefits of implementing an off-the-shelf solution. While Defence made necessary configuration changes to the off-the-shelf system to accommodate business needs, Defence retained the integrity of the system for future upgrades. Defence also intended that the system would automatically capture civilian health care provider referrals and reporting; support dispensing of pharmaceuticals; and exchange information with Defence's financial management and accounting system. However, this work was not progressed, which has delayed the implementation of agreed DeHS functionality and the realisation of intended benefits.¹³

13 In December 2014, Defence informed the ANAO that functional specifications have been developed and a design document is being prepared for the introduction of a dispensing management module.

23. The ANAO interviewed clinical practitioners and practice managers from two health centres some six months after site rollout, and found general acceptance of DeHS from most Defence health groups. These health groups reported better patient care with access to a single patient eHealth record.¹⁴ However, stakeholders also considered there were issues requiring attention, including system performance, delays in accessing templates and longer clinical consultation periods for several health groups. DeHS is a complex system that requires ongoing management to avoid risks to business processes and technical functionality.

24. Prior to the implementation of DeHS, JHC had identified that business processes were not uniform across health centres. In consultation with health groups, JHC developed standardised business processes for the use of DeHS to support Defence's clinical service delivery model. However, pockets of clinical practitioners elected to revert to prior business practices. The adoption of past practices does not provide a uniform basis for accurate reporting of clinical and health trends—an aid to the efficient delivery of health care services. As with any major ICT and business reform, successful implementation relies on cultural acceptance and behaviour change, and Defence should maintain an ongoing focus on stakeholder consultation as well as remediation to help realise intended benefits of the system.

Lessons learned and recommendations

25. As discussed, Defence's management of the DeHS project was beset, in its early phases, by a range of avoidable shortcomings. A key lesson of this audit is the importance of properly scoping and planning complex ICT projects, as a basis for providing sound advice to Defence senior leadership and government, and establishing the pre-conditions for successful implementation. There are more restricted options for Defence senior leadership and government once a project that is considered beneficial is well underway and clearly requiring funds beyond its original budget. This underlines the critical importance of applying a rigorous approach at the outset of a project to develop the project scope and budget. Project proposals and cost estimates should be based on a full understanding of project parameters and risks, and subject to thorough review.

14 For example, registered nurses and physiotherapists found the ability to review clinical consultation notes valuable when planning patient treatments, while practice managers indicated they could follow up on missed patient appointments and schedule staff rosters 12 months in advance.

26. A further lesson of the audit is the importance of adequate coordination of internal resources and expertise—to mitigate project risks and inform effective delivery—and the adoption of sound project management methodologies and practices. Government has endorsed project management methodologies so that entities follow a structured approach in developing, overseeing and delivering intended capability, and these methodologies should be consistently followed.¹⁵ Further, Ministerial approvals, and processes such as Gateway reviews, are specified by government to oversight the effective use of public resources so as to achieve value for money in project delivery, and Defence is expected to apply these requirements.

27. The ANAO has made two recommendations aimed at providing Defence with reasonable assurance that project proposals and cost estimates are reliable; and achieving benefits realisation for DeHS by standardising use of the system and implementing agreed functionality.

Summary of entity response

28. The Department of Defence provided the following summary response, with the formal response at Appendix 1:

29. Defence acknowledges the findings contained in the audit report on the Electronic Health Records for Defence Personnel and agrees with the two recommendations.

30. Since the implementation of Defence eHealth System (DeHS), Defence has made significant improvements in the assurance of ICT projects. In particular, improvements in the governance of approval processes and the establishment of professionalization streams have reinforced the internal accountabilities. These accountabilities ensure future adherences to approved project management methodologies, ministerial approval and Gateway Review processes.

31. Defence thanks the ANAO for the insights provided regarding the system implementation of DeHS, and will incorporate the issues identified in the audit with the continued use of DeHS.

15 The UK Office of Government Commerce (OGC) guidance *Managing Successful Programmes* (MSP) and *Prince2* are two endorsed methodologies for managing complex programs and projects.

Recommendations

**Recommendation
No. 1****Paragraph 2.46**

To provide reasonable assurance that complex ICT project proposals and cost estimates are reliable, the ANAO recommends that Defence reinforce the internal accountabilities necessary to:

- (a) properly scope, cost and validate project proposals; and
- (b) adhere to approved project management methodologies, ministerial approval and Gateway Review processes.

Defence's response: *Agreed*

**Recommendation
No. 2****Paragraph 3.82**

To achieve benefits realisation, the ANAO recommends that Defence:

- (a) evaluate stakeholders' use of DeHS and reinforce standardised business processes; and
- (b) finalise post-implementation planning, including by identifying resources and a timetable to implement agreed DeHS functionality.

Defence's response: *Agreed*

Audit Findings

1. Introduction

This chapter provides an overview of the Defence Electronic Health System. It also introduces the audit, including the audit objective, criteria and approach.

Overview of the Defence Electronic Health System

1.1 The Department of Defence (Defence) provides health care services to some 80 000 Australian Defence Force (ADF) personnel throughout their service, from their induction until their discharge. ADF personnel move regularly during their military service, for postings and deployments, and they receive health care services through both military and civilian channels. The number of serving personnel, their multiple locations, mobility, and access to different channels for health care increase the complexity of maintaining complete, accurate and up to date medical records. An effective electronic health (eHealth) system assists in maintaining medical records, delivering integrated health care, and in providing valuable information to stakeholders on health care services and the health of personnel.

1.2 In May 2009, Defence finalised a business case to deliver a contemporary health records management system for ADF personnel. The proposed system was originally called the Joint eHealth Data and Information System (JeHDI) and was later known as the Defence eHealth System (DeHS).¹⁶ The business case noted that the proposed system would centralise, electronically capture and manage ADF health records, and seamlessly link health data for ADF personnel. The system was also to be used to help assess the preparedness of ADF personnel for operations, and inform health groups¹⁷ preparing for deployment in support of operations.

1.3 In February 2010, Defence approached the market seeking tenders for a proven eHealth system to meet its business requirements. CSC Australia Pty Ltd (CSC)¹⁸ was awarded the contract to implement an off-the-shelf product sourced from Egton Medical Information Systems, a United Kingdom (UK)

16 The project is referred to as DeHS throughout this audit report to be inclusive of both the business solution and the enabling ICT system.

17 The ADF refers to clinicians, dentists, nurses and other allied health providers as members of craft groups. These groups are referred to as health groups throughout this audit report.

18 Defence awarded a contract to CSC Australia Pty Ltd (CSC) to build, host and support Defence's eHealth System through to 2019–20 at a value of \$68.9 million; and awarded a \$6.1 million contract for project management services to IT services provider Oakton.

firm. The product was known as the Primary Care System (EMIS PCS)—an eHealth system used by the UK Ministry of Defence (MoD).¹⁹

1.4 When announcing the system development contract, the then Minister for Defence Science and Personnel outlined the main purpose of the new system, stating that '[DeHS] will link health data from recruitment to discharge and allow for treating health practitioners to access a patient's complete health record'. He described DeHS as 'a web based system which can be accessed wherever Internet is available, while still maintaining confidentiality and data integrity'.²⁰

1.5 The DeHS project has been managed by Defence's Joint Health Command (JHC)²¹, with the system designed, built, hosted and supported by CSC. By December 2014, DeHS was deployed and in use across Defence's Garrison Health environments. Deployment of DeHS for use in operational environments, such as on board ships, remained a planned activity.

DeHS funding approvals and basis

1.6 The Chief of the Defence Force (CDF) and Secretary of Defence approved acquisition and sustainment funding of \$23.3 million in June 2009 to develop DeHS in a staged approach: from prototype to pilot, and on to a mature production system by December 2011. There was an expectation at the time that the system would be hosted and managed internally as part of the Defence ICT environment, which meant that the resources applied to support Defence's extant eHealth systems could eventually be used to support the new system.

1.7 Since 2009 there have been two major increases to the original DeHS acquisition and sustainment budget of \$23.3 million, resulting from changes to project scope:

- In November 2010, the Minister for Defence sought concurrence from the Finance Minister for approval of the DeHS project, including

19 In May 2006, the military version of EMIS PCS was selected by MoD as part of the Defence Medical Information Capability Programme (DMICP). The system has been implemented and is reported to support over 16 000 consultations per day.

20 The Hon. Warren Snowdon MP, Minister for Defence Science and Personnel, 'JeHDI Helping Shape eHealth Future', media release, Parliament House, Canberra, 9 February 2011.

21 As part of the Vice Chief of Defence Force (VCDF) Group, JHC develops strategic health policy, provides strategic level health advice and exercises technical and financial control of ADF health units.

significantly higher project costs.²² The Finance Minister agreed to the commencement of final contract negotiations with CSC, conditional on the then Department of Finance and Deregulation (Finance) agreeing to final project costs prior to Defence signing the contract. In January 2011, Finance agreed to total project costs of \$85.9 million, comprising \$54.6 million for acquisition costs and \$31.3 million for sustainment costs from 2010–11 to 2019–20.

- In February 2014, Defence obtained approval from the National Security Committee of Cabinet to increase the DeHS budget by a further \$47.4 million to address capability shortfalls, including for the purchase of additional software licences and to fund training requirements.

1.8 Over time, the approved total DeHS project cost rose to \$133.3 million, some \$110.0 million higher than the original budget. At each approval stage, the project has been funded internally using Defence’s departmental budget, and Defence did not request supplementary funding from government. Nevertheless, there is an opportunity cost associated with Defence allocating significant additional funds to the project. Table 1.1 provides a summary of DeHS funding approvals since 2009, and the principal reasons for the increase in costs.

22 Defence projects valued from \$20 million to \$100 million required the approval of both the Minister for Defence and Minister for Finance, and those valued at \$100 million or more required the approval of Cabinet.

Table 1.1: DeHS funding approvals and basis of costings

Approval date	Acquisition (\$ million)	Sustainment (\$ million)	Total (\$ million)	Costing basis and reasons for change
June 2009	20.5	2.8	23.3	a) Sustainment period to 2018–19. b) System hosted and managed internally in Defence's ICT environment. • <i>Not costed: deployment; re-assignment of staff from Defence's extant Health systems to support DeHS.</i>
January 2011	54.6	31.3	85.9	a) Sustainment period to 2019–20. b) System hosted and supported externally by CSC.
February 2014	84.5	48.8	133.3	a) Sustainment period to 2019–20. b) System hosted and supported externally by CSC. • <i>Additional funding for: software licences; training requirements; hardware, infrastructure and enhancements.</i>

Source: ANAO.

1.9 In summary, the principal reasons for the increase in DeHS project costs were: a one year extension of the funded sustainment period; hosting the system externally rather than internally; and the inclusion of previously unbudgeted items such as training requirements.

1.10 In light of concerns about cost overruns, shortcomings in Defence's project planning and the quality of the project proposals brought forward to government, the Treasurer requested that the Auditor-General consider undertaking a performance audit of the processes used by Defence in its development of DeHS. The Auditor-General agreed to the Treasurer's request.

DeHS features and potential benefits

1.11 The key features of DeHS are:

- a *Primary Care System* (PCS)—an eHealth care system used to record all clinical, dental, mental health and allied health consultations, treatments and findings;
- *DeHS Access*—an online patient-accessible summary of each patient's eHealth record; and
- *DeHS Reporting*—a suite of reporting tools available to report on individual or corporate information requirements.

1.12 These three features of DeHS are intended to operate together to provide a clinical management tool that enables safe and quality health care for the ADF member. The system design provides for health groups and Defence to refer to the health information contained within DeHS to enable evidence based decision making. The DeHS business case also noted that the system would:

- inform ADF Commanders of the readiness for operational deployments of individuals and Force Elements;
- contribute to the generation of health performance and work health and safety (WHS)²³ metrics to support the management of resources, planning and accountability; and
- provide for effective health management after an ADF member's discharge. For example, the health record of an ADF member would be transferred or accessed by the Department of Veterans' Affairs as part of ongoing care and/or to inform compensation determinations.

1.13 Table 1.2 summarises the anticipated benefits of DeHS.

23 Revised work health and safety (WHS) laws commenced on 1 January 2012 in many states and territories to harmonise occupational health and safety (OH&S) laws across Australia.

Table 1.2: DeHS anticipated benefits

Key focus areas	
ADF personnel / customer	
Health readiness	<ul style="list-style-type: none"> • Reduced morbidity through improved personal health management. • Increased personnel available for deployment through more accurate and timely reports. • Faster Medical Employment Classification (MEC)^A upgrades through better coordinated care. • Faster force health preparation through better availability of information.
Productivity	<ul style="list-style-type: none"> • Reduced waiting time for individual consultations. • Reduced cancellations and re-bookings. • Reduced time lost through shorter episodes of care. • Reduced time lost through more effective rehabilitation programs.
Defence health	
Productivity	<ul style="list-style-type: none"> • Reduced clinician time spent on administration, recording patient history, bookings, patient administration, referrals and reports. • Reduced clinician time spent on improving practice workflow. • More efficient use of pharmaceuticals and medical consumables. • More efficient external contractor sourcing. • More effective and efficient response to ministerial and other external enquiries. • Reduced storage requirements for paper-based records.
Quality of care	<ul style="list-style-type: none"> • Earlier identification and management of individual health problems. • Improved clinical decisions. • Fewer adverse drug events and clinical errors. • Fewer duplicated tests and referrals. • Shorter episodes of care and faster rehabilitation. • More effective clinical compliance monitoring. • More effective and efficient professional accreditation and provider credentialing.
Population health	<ul style="list-style-type: none"> • Earlier identification and control of infectious disease outbreaks. • Earlier identification and management of non-communicable disease clusters. • Earlier identification and control of occupational injury hazards. • More effective evidence-based health policies and programs. • More effective and efficient health research.
Other entities	
Claims assessment	<ul style="list-style-type: none"> • Faster health records access. • Faster and more accurate entitlements assessment. • Reduced storage requirement and handling costs for paper-based records.
Veterans' health	<ul style="list-style-type: none"> • More effective and efficient veterans' health studies.

Source: ANAO analysis of Defence's business case for an eHealth information system.

Note A: The Medical Employment Classification (MEC) system provides a consistent tri-Service approach to the application of medical fitness standards in the employment of Defence members.

Longer term benefits

1.15 While the primary focus for DeHS is to provide a clinical health management tool which centralises, electronically captures and manages ADF health records, Defence intends to progressively extend the system's functionality as part of other Defence projects. In particular, the ADF Deployable Health Capability (JP2060) project is to deliver health capability across operational environments; and the Defence Management Systems Improvement (JP2080) project is to improve the functionality of Defence's corporate support systems and the interchange of information between systems.²⁴

1.16 More broadly, the National eHealth Strategy provides a strategic framework and plan to guide national coordination and collaboration in eHealth.²⁵ DeHS is intended to align closely with the guidance contained in the strategy and with the eHealth standards and specifications developed by the National eHealth Transition Authority (NEHTA). These standards and specifications provide for interconnectivity between health information systems.

1.17 DeHS is also expected to link with the national Personally Controlled Electronic Health Record (PCEHR)²⁶, which is being implemented by the Department of Health as part of the National eHealth Strategy. More specifically:

[DeHS] is building the capability to interact with the national Personally Controlled Electronic Health Record (PCEHR) for the interchange of health information across private and public health systems. Members will be able to

24 JP2060 is a multi-phase joint project which involves the identification and development of capabilities required to prevent, treat and evacuate casualties in joint operations in the defence of Australia and its interests. JP2080 is another joint project intended to enhance Defence's core financial and personnel information systems to accommodate changes in user requirements, technical platforms and upgrades to the commercial applications on which they are based.

25 The Strategy was commissioned by the Australian Health Ministers' Advisory Council and released in December 2008.

26 PCEHR is envisaged to be an:

electronic health record for Australians, [which] will be a reliable, secure and trustworthy source of key clinical information. It will facilitate efficient and effective treatment of patients by health practitioners and enable consumers to access and manage their own health records in cooperation with their health providers to improve care. It will respect individual privacy but be clinically valuable to all areas of the health care industry. Interaction with the electronic health record will be highly automated and form a natural part of clinical workflows. The value of sharing health information electronically between healthcare professionals, will be demonstrated by enhanced efficiency and effectiveness of the delivery of healthcare, reduced hospitalisations and ultimately lives saved.

Department of Health, *Review of the Personally Controlled Electronic Health Record*, December 2013, p. 1, available from <<http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth>> [accessed 21 May 2014]

consent to participation in the PCEHR system while in Defence or when they discharge.²⁷

Related reviews and audits

1.18 The catalyst for DeHS dates back to 1989 when the Defence Regional Support Review identified the need to centralise and computerise ADF health records. Since that time other reviews and ANAO performance audits have identified shortcomings in Defence's management of ADF health services.²⁸

1.19 ANAO Audit Report No.49 of 2009–10, *Defence's Management of Health Services to Australian Defence Force Personnel in Australia*, highlighted inadequacies in electronic medical records management for serving personnel. The ANAO noted that:

Defence does not currently have effective information and patient records systems to support the delivery of ADF health services. These systems are needed to help realise efficiencies (for example, through the provision of better management information) in the provision of appropriate health care for ADF members.

Defence has previously attempted to introduce a patient records system, the Health Key Solution or HealthKeyS. However, users found HealthKeyS difficult to use (for example, moving between different screens is not easy and the system has poor response times). For this reason, only some health facilities currently use HealthKeyS and Defence has now decided to introduce a replacement system which is currently under development. A lesson learned from the failure of HealthKeyS is the need for the system to meet user needs. Defence expects to progressively deploy its replacement system, to be developed based on commercial off-the-shelf products and to be called the Joint e-Health Data Information system, between July 2011 and December 2013.²⁹

27 Senate Standing Committee on Foreign Affairs, Defence and Trade, Senate Budget Estimates 28–29 May 2012, Defence answer to Question on Notice No.119, available from <http://www.aph.gov.au/~media/Estimates/Live/fadt_ctte/estimates/bud_1213/def/Department-of-Defence/Defence_QONs.aspx> [accessed on 5 June 2014].

28 For further details, see: Devolution and integration in the Australian Defence Force: the Defence Regional Support Review (1989); ANAO Audit Report No.34 1996–97, *Australian Defence Force Health Services*; Future directions for the management of Australia's defence—Report of the Defence Efficiency Review (1997); ANAO Audit Report No.51 2000–2001, *Australian Defence Force Health Services Follow-up Audit*; Review of Defence Health Services (Stevens Review, 2004); Healthcare in the Australian Defence Force (Alexander Review, 2008); Senate Committee for Foreign Affairs, Defence and Trade inquiry into Australia's Involvement in Peacekeeping Duties (2008); and Review into Mental Health in the ADF (Dunt Review, 2009).

29 ANAO Audit Report No.49 2009–2010, *Defence's Management of Health Services to Australian Defence Force Personnel in Australia*, p. 25.

1.20 Defence's Audit Branch conducted internal audits of DeHS as part of its 2011–12³⁰ and 2012–13³¹ Audit Work Programs, the second internal audit was initiated by JHC. The first audit focused on key controls in connection with the management of health care data, including privacy management, data conversion, archiving of data and compliance with relevant data management standards and legislation. The audit observed that:

Audit expected planning and project documentation to be more advanced than was observed during the review. This is particularly relevant to the security design, data migration process and benchmarking of compliance against legislation (being privacy and records management legislation). Given the extreme reputational exposure from failure to manage security, privacy and data accuracy in connection with healthcare records, and the short time frame to implement the system (less than five months), priority must be given to address these issues.

1.21 During the first internal audit, Defence management requested that the Audit Branch extend the scope of its review to examine project management processes, including financial management and business implementation. The second internal audit responded to the request and observed that as at November 2012:

Analysis of the overall financial status of the projects indicates that the:

- approved budget was underestimated by approximately \$8.4 million³²;
- project contingency is overspent by \$2.2 million with no unallocated contingency funds available for 2013–2020;
- overall costs (e.g. Full Time Equivalent (FTE) costs and rental costs) associated with the implementation of the [DeHS] system are not being costed and tracked.

1.22 The internal audit report also expressed concern that DeHS may not realise intended business benefits:

The full benefit of [DeHS] will be only realised if it is continuously updated with up to date health records. However, the current architecture does not support this

30 Defence Audit Branch, Audit Task No.12–029, *Implementation of Joint eHealth Data—Phase 1*, October 2012.

31 Defence Audit Branch, Audit Task No.13–046, *Implementation of Joint eHealth Data—Phase 2*, November 2012.

32 ANAO comment: The \$8.4 million budget shortfall was in relation to the \$85.9 million project funding approved in January 2011.

as the [DeHS] system will only be implemented in the garrison environment. It will not be available in the deployed environment or aboard Navy vessels. At this time, business processes have not been established to continuously update the [DeHS] system in instances where the system is unavailable.

The relatively tight timeframe to achieve key milestones and the readiness of Joint Health Command (JHC) to support the implementation increases the risk that the eHealth capability will not be achieved with a November 2012 implementation. Therefore, it is critical for JHC to reschedule system implementation to a timeframe which will ensure business acceptance of the system.

About the audit





1.23 The objective of the audit was to examine the effectiveness of Defence's planning, budgeting and implementation of an electronic health records solution for Defence personnel. The scope of this audit covered the development and implementation phases of DeHS from project inception in 2009 through to the end of 2014, and included a focus on the quality of Defence's advice to government.

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

- Defence adequately defined DeHS business requirements;
- Defence developed an appropriate DeHS project scope and budget, and adhered to government procurement policies and procedures;
- DeHS project governance and management supported effective system implementation, and the design and build of DeHS delivered intended functionality;
- DeHS maintains the security and integrity of health information; and
- Defence established standardised eHealth processes through the use of DeHS.

1.25 To assess the effectiveness of Defence’s administration of DeHS, the ANAO developed a grading scheme, as illustrated in Table 1.3.





Table 1.3: Grading scheme for assessing effectiveness

Grading scheme	
	Limited effectiveness—delivered minimal outcomes.
	Partially effective—delivered some of the outcomes.
	Generally effective—delivered most of the outcomes.
	Effective—delivered outcomes.

Source: ANAO.

1.26 The ANAO’s assessments in terms of the audit criteria, as at 2014–15, are included in the body of the report, with a consolidated table of assessments presented in Appendix 2. The assessments are presented in the format illustrated in Table 1.4.

Table 1.4: Assessment of effectiveness against criteria

Criteria	Assessment of effectiveness			
Define business requirements				
Assess business requirements.				
Adopt a proven system.				
Scope, budget and procure				
Supply business requirement.				
Budget and approval.				
Shape the system to meet business requirements.				
Project manage and implement				
Establish management arrangements.				
Build ICT environment.				
Connect with extant systems.				
Gain system assurance.				
Deploy and maintain ICT system.				
Security and integrity of information				
Migrate data from extant systems.				
Consolidate data into a single record.				
Maintain and review data security and integrity.				
Deliver standardised business processes				
Assess extant processes to inform standardised business processes.				
Explain the standardised business processes and ICT system.				
Identify and address shortfalls, and make changes to better the system.				

Source: ANAO.

1.27 The audit fieldwork was conducted between July and September 2014. The ANAO:

- reviewed Defence's project documentation and government submissions;
- interviewed key business stakeholders, including Defence and other Australian Public Service personnel, medical and allied health staff, and contractors involved in the delivery of the project;
- reviewed implementation of the agreed recommendations in Defence's two internal audits; and

- examined user access controls and administrative privileged accounts that support the integrity of the information system.

1.28 The audit was conducted in accordance with the ANAO's auditing standards, at a cost to the ANAO of approximately \$316 000.

Structure of the report

1.29 The structure of the report is as follows:

- Chapter 2 examines Defence's planning and procurement processes for DeHS. It also outlines the typical steps for accessing eHealth records from DeHS.
- Chapter 3 examines Defence's project management and implementation; the security and integrity of information maintained in DeHS; and the development of standardised DeHS business processes.

2. Planning and Procurement

This chapter examines Defence's planning and procurement processes for DeHS. It also outlines the typical steps for accessing eHealth records from DeHS.

Introduction

2.1 The effective development of complex ICT project proposals depends on a structured approach: to engage resources and expertise; identify business requirements, project scope and key risks; and provide reasonable assurance that proposals and cost estimates are reliable. A sound planning approach also informs the procurement process, and the identification of a system that is 'fit for purpose' to deliver intended functionality and achieve outcomes.

2.2 In this chapter, the ANAO examines Defence's:

- definition of DeHS business requirements; and
- DeHS project scope, budget and procurement.

Defining business requirements

2.3 A business case should be prepared with due consideration given to business requirements, as a first step towards acquiring or developing a system that is fit for purpose. Before the development of the DeHS business case in 2008–09, Defence had experienced deficiencies in the collection, quality and reporting of health care information over a 15 year period. Following two unsuccessful earlier attempts to implement an eHealth system³³, Defence intended to introduce a contemporary health records management system for ADF personnel.

Summary assessment

2.4 To assess Defence's overall effectiveness in defining DeHS business requirements, the ANAO examined whether:










- the DeHS business case was informed by a formal analysis of business requirements;

33 HealthKeyS and MIMI were two competing and discrete Defence eHealth systems that did not meet clinical user needs or Defence's management requirements.

- business requirements addressed patient and health group needs, management reporting and the sharing of information between Defence and other health services;
- Defence was mindful of the lessons learned from implementing extant eHealth systems, including any shortcomings, and the need for a fit for purpose system;
- the business case considered a proven ‘off-the-shelf’ solution;
- the business case aligned with Defence’s eHealth strategy and the National eHealth Strategy; and
- consideration was given to the National eHealth Transition Authority (NEHTA) standards and specifications.

2.5 Table 2.1 provides a summary assessment of Defence’s overall effectiveness in defining DeHS business requirements. The table shows the state observed by the ANAO as at September 2014; and the planned state as anticipated by Defence by March 2015.

Table 2.1: Summary assessment of Defence’s effectiveness in defining DeHS business requirements

Criteria	Assessment of effectiveness
Define business requirements	
Assess business requirements.	
Adopt a proven system.	
KEY:	<p>Limited effectiveness—delivered minimal outcomes </p> <p>Partially effective—delivered some of the outcomes </p> <p>Generally effective—delivered most of the outcomes </p> <p>Effective—delivered outcomes </p> <p> Observed state at September 2014</p> <p> Defence's planned state by March 2015</p>

Source: ANAO analysis.

Assessing business requirements

2.6 During the development of the DeHS business case, JHC consulted key representatives from health groups and support services—such as the Chief Information Officer Group—to better understand current and emerging business needs in the Garrison Health and Defence ICT environments. JHC also consulted the then Department of Health and Ageing and the Department of Veterans’ Affairs to define and validate the business need and system requirements necessary to support the National eHealth agenda.

2.7 The business case identified that extant Defence eHealth information systems were well below contemporary Australian practice; and there were no means to effectively facilitate multi-discipline exchange of health, mental health, epidemiological, management and work health and safety (WHS) information. As a consequence, there was a risk that some ADF members were receiving sub-optimal care. The business case also identified risks for the transition to DeHS, including the need to manage multiple eHealth systems, the requirement to redevelop disparate health processes into standardised business processes, and reputational risks should Defence encounter shortcomings in deploying an eHealth system.

2.8 The business case noted that the proposed system would:

- centralise, electronically capture and manage ADF health records, and seamlessly link health data for ADF personnel;
- assist the preparation of ADF personnel for operations, and the preparation of health groups for deployment in support of operations;
- initially be deployed in the Garrison Health environment, and later deployed in the Defence operational environment; and
- comply with national and international standards for eHealth systems.

2.9 While the business case identified business requirements and key risks, it was also somewhat ambitious. Defence planned to: aggregate patient health records from multiple Defence systems; standardise business processes across all health groups at the same time Defence was redesigning its health services support model, including its contractual arrangements; and deploy DeHS in operational environments.³⁴ However, the business case lacked detail on how these requirements would be achieved.

Adopting a proven system

2.10 Following the 2008 ADF Health Services Review, the then Commander Joint Health recommended the investigation of a commercial or military ‘off-the-shelf’ eHealth informatics system that could fast track Defence’s system

³⁴ In June 2012, the then Minister for Defence Science and Personnel announced a new \$1.3 billion contract between Defence and Medibank Health Solutions (MHS) to provide health care services to ADF personnel across Australia. The MHS agreement is for an initial four year term, delivering a broad range of services, including on-base health support, pathology, imaging and radiology and a 24-hour ADF national health hotline.

requirements. In September 2008, Defence's Rapid Prototyping, Development and Evaluation (RPDE) program was tasked to investigate the availability of off-the-shelf products, and to confirm Defence's business case through a proof of concept. The RPDE Report identified several off-the-shelf products that would support Defence's business needs.

2.11 The May 2009 DeHS business case noted that a number of mature and immediately available off-the-shelf products could be integrated to form the basis of the proposed system. The business case also indicated 'the capability proposal is well aligned to the existing need and can work with legacy ADF systems such as HealthKeyS, PMKeyS and ROMAN.'³⁵

Project scope, budget and procurement

2.12 Having established the DeHS business case, Defence commenced work on a procurement process for the system. That process confirmed the availability of a suitable 'off-the-shelf' system, and led to changes in the project scope and budget. Defence approved project funding internally in June 2009, sought government approval of the DeHS project during the procurement process in November 2010, and later sought government approval of additional project funding in February 2014.

Summary assessment

2.13 To assess Defence's overall effectiveness in scoping, budgeting for and procuring DeHS, the ANAO examined whether:

- business and functional requirements appropriately informed the procurement process;
- the procurement process adhered to government and Defence procurement policies and procedures;
- an accurate budget—to procure, implement and sustain the system—was prepared and formally approved;
- DeHS is fit for purpose as an 'out-of-the-box' solution and configurable to accommodate specific Defence requirements;

³⁵ HealthKeyS was Defence's extant eHealth system and was partially deployed in Garrison Health environments in Queensland and South Australia; PMKeyS is Defence's enterprise human resource management information system; and ROMAN is its financial management and accounting system.

- additional functionality can be introduced with nominal ICT system changes; and
- DeHS can interface with extant information systems.

2.14 Table 2.2 provides a summary assessment of Defence’s overall effectiveness in scoping, budgeting for and procuring DeHS. The table shows the state observed by the ANAO as at September 2014; and the planned state as anticipated by Defence by March 2015.

Table 2.2: Summary assessment of Defence’s effectiveness in scoping, budgeting for and procuring DeHS

Criteria	Assessment of effectiveness			
Scope, budget and procure				
Supply business requirement.				
Budget and approval.				
Shape the solution to meet business requirements.				
KEY:	<div><div>Limited effectiveness—delivered minimal outcomes</div><div>Partially effective—delivered some of the outcomes</div><div>Generally effective—delivered most of the outcomes</div><div>Effective—delivered outcomes</div></div>			
Observed state at September 2014				
Defence's planned state by March 2015				

Source: ANAO analysis.

Supplying business requirements

2.15 A well prepared and comprehensive business case informs the procurement process. Tender documentation needs to clearly express business and functional requirements for potential suppliers, and the criteria to be used to assess tender proposals.

2.16 Following the development of the DeHS business case, in June 2009, JHC submitted a proposal to the CDF and Secretary of Defence seeking approval to commence the DeHS project in the first quarter of 2009–10. The proposal advised that:

- Defence’s extant eHealth systems were below contemporary Australian practices;
- ‘off-the-shelf’ products were available that could interface with Defence ICT systems and other information systems;
- further delays to implement an eHealth system posed risks to Defence’s reputation; and

- DeHS had many potential benefits and would help shape the National eHealth agenda.

2.17 The CDF and Secretary of Defence approved acquisition and sustainment funding for DeHS in June 2009 at a cost of \$23.3 million. JHC then commenced work on the DeHS procurement process. Defence released an open approach to the market in February 2010. The Request for Tender statement of work reflected the DeHS business case in detailing the required high level functionality of the system³⁶:

- *Clinical care*—support the assessment and treatment of patients and the provision of health care within Defence;
- *Practice management*—support the coordination and operation of the health care providers' business;
- *Health management and reporting*—support overall health management and reporting for analysis and management needs; and
- *Interface with systems*—interface with other Defence and NEHTA-compliant systems.

2.18 To better assist the market in understanding Defence's complex business and technical environments, the statement of work also provided background information on the business and service delivery model for JHC, an overview of the Defence computing environment, and the proposed system architecture and information management lifecycle. Overall, Defence made significant effort to inform the market of the proposed concept of operations for DeHS, the functional and performance specifications for the system, and the business and operational scenarios the system must support.

2.19 Five companies responded to the tender, each with international experience in designing, building, implementing and hosting an eHealth system. The tender evaluation team assessed the tenders against the evaluation criteria and shortlisted two companies to conduct negotiations for best and final offers. This process led to the selection of CSC as the preferred tenderer on the basis that it offered a robust and proven (off-the-shelf) solution that represented value for money and reduced financial, corporate and legal risks.

36 The Request for Tender was prepared using *ASDEFCON (Complex Materiel)* Volume 2—a suite of Defence contract templates that, in broad terms, outlines the requirements for the proposed system and services to support the system.

2.20 CSC was awarded the contract to implement an off-the-shelf product sourced from Egton Medical Information Systems, a United Kingdom (UK) firm. The product was known as the Primary Care System (EMIS PCS)—an eHealth system used by the UK Ministry of Defence (MoD). The military version of EMIS PCS was selected by MoD in May 2006 as part of the Defence Medical Information Capability Programme. The system has been implemented by the MoD and is reported to support over 16 000 consultations per day. In the early phases of the DeHS project, then Commander Joint Health and project staff discussed the UK experience of EMIS PCS with MoD colleagues. Defence sought reassurance from its discussions with MoD that EMIS PCS was ‘fit for purpose’ and would only require configuration changes.

2.21 The final negotiated contract price with CSC was \$68.9 million for the period 2010–11 through to 2019–20. This included initial build costs of \$30.0 million; infrastructure and software rental costs of \$16.0 million; managed support of \$18.6 million from 2015–16 to 2019–20; and EMIS licencing costs of \$4.2 million.

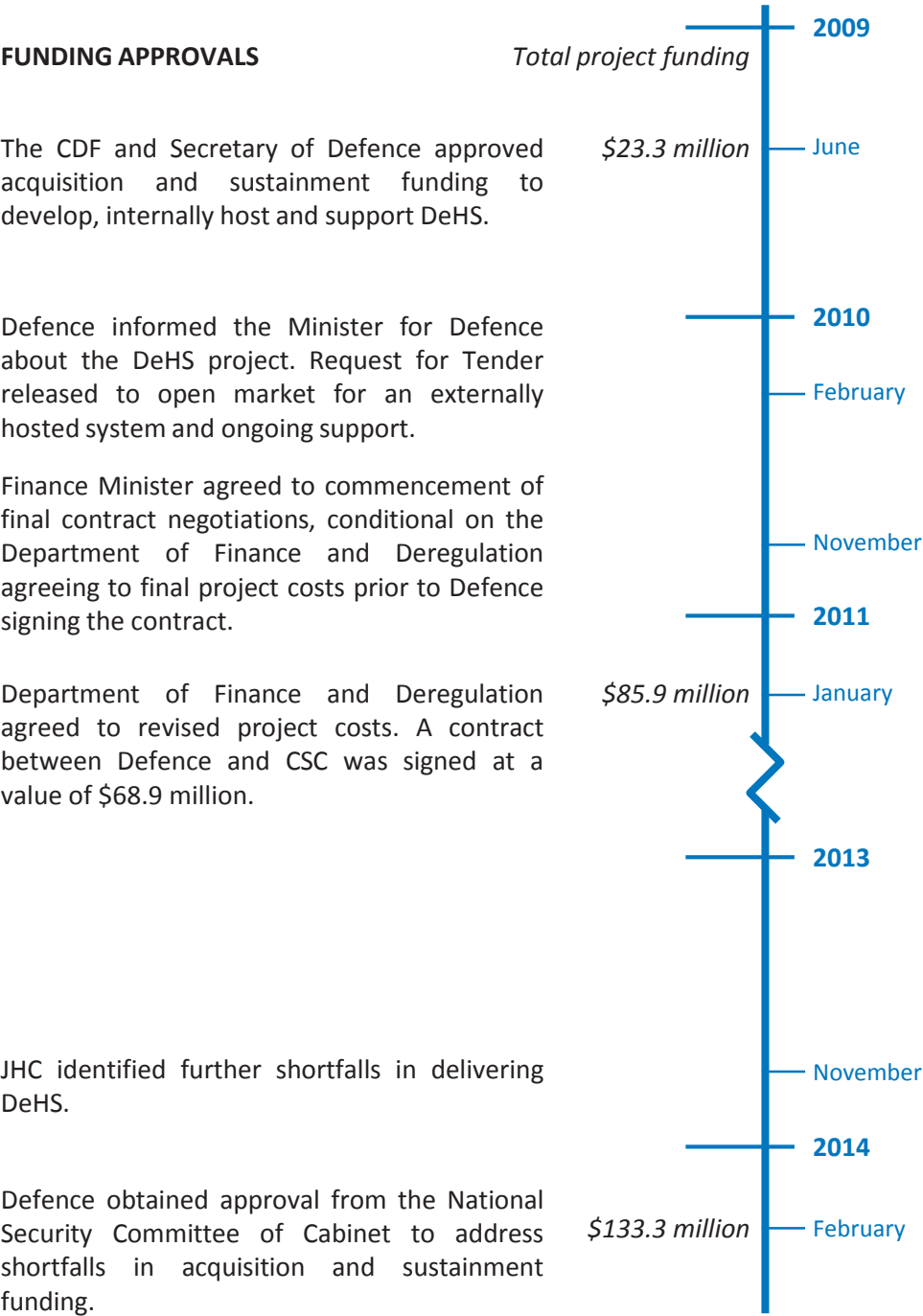
Budget and approval

2.22 As discussed, the CDF and Secretary of Defence approved acquisition and sustainment funding of \$23.3 million in June 2009, and by January 2011 the final negotiated contract price with CSC was \$68.9 million.³⁷

2.23 Over the course of the project, Defence developed a better understanding of the project scope and the associated costs, which led to government approval of additional project funding on two occasions. The project budget increased to \$85.9 million in January 2011 and again to \$133.3 million in February 2014, some \$110 million higher than the original budget. The funding approvals are illustrated in Figure 2.1 and discussed in the following paragraphs.

37 The CSC contract price did not represent the full project cost, which also included project management and contingency costs.

Figure 2.1: DeHS project funding approvals



Source: ANAO.

2.24 The June 2009 DeHS project proposal did not include funding for progressive deployment of the system in the Garrison Health and operational environments. The proposal instead made the assumption that savings from Defence's Strategic Reform Program (SRP)³⁸ remediation activities would fund full deployment across the Garrison Health environment, and that the program to establish the ADF Deployable Health Capability (JP2060)³⁹ would fund deployment in the operational environment. However, Defence did not determine the level of funding required from these alternate sources, and the absence of costing detail in the proposal was not identified as a concern.

2.25 Further, Defence did not identify in June 2009 that the project required ministerial rather than departmental approval because it exceeded the financial threshold for ministerial approval of \$20 million.⁴⁰ Defence first informed the then Minister for Defence about the DeHS project in February 2010, before releasing the Request for Tender. However, Defence informed the Minister that the estimated cost of the project was \$19 million when the approved cost was actually \$23.3 million.⁴¹

2.26 Defence's approach to market in February 2010 differed from the DeHS business case in that it sought bids for an externally hosted system and ongoing support, rather than an internally hosted system. This change in direction had significant implications for the project's scope and budget, and it was not approved by Defence senior leadership prior to commencing the procurement process.

2.27 In November 2010, the Minister for Defence sought concurrence from the Finance Minister for approval of the DeHS project, including significantly higher project costs. The Finance Minister agreed to the commencement of final contract negotiations with CSC, conditional on the then Department of Finance and Deregulation (Finance) agreeing to final project costs prior to Defence signing the contract.

38 On 2 May 2009 the then Government launched both the 2009 Defence White Paper and the SRP. Defence expected the SRP to improve accountability, planning and productivity and deliver savings of \$20 billion over the decade 2009–10 to 2018–19.

39 See footnote 24.

40 Defence projects valued from \$20 million to \$100 million required the approval of both the Minister for Defence and Minister for Finance, and those valued at \$100 million or more required the approval of Cabinet.

41 See paragraph 2.23.

2.28 A key matter raised by the Finance Minister was the conduct of a Gateway Review for the project. These independent reviews are normally conducted for all IT projects valued at over \$10 million, and are intended to identify and focus on issues of most importance to a project, so that the project team's effort is directed to those aspects that will help the project be successful.⁴² However, the Finance Minister pointed out that in the case of DeHS:

the project has progressed too far for the Gateway Review Process to add value, even though the Gateway team has indicated that [DeHS] would have benefited from the review process.⁴³

2.29 It is not evident from Defence records why a Gateway Review was not undertaken. The subsequent history of the DeHS project indicates that the decision not to proceed with a Gateway review was an opportunity lost.

2.30 In January 2011, the then Department of Finance and Deregulation (Finance) agreed to project costs of \$85.9 million, including \$54.6 million towards acquisition costs and \$31.3 million for sustainment costs from 2010–11 to 2019–20. The increase in project costs was to be funded internally using Defence's departmental budget. The contract between Defence and CSC Australia was signed on 13 January 2011 at a value of \$68.9 million. The difference between the total project costs of \$85.9 million and the value of the CSC contract (\$68.9 million) mostly comprised project management services (provided by Oakton), and project contingency funding.

2.31 By November 2013—during the fifth year of the project and on the eve of commencing the implementation phase—JHC identified further impediments to delivering DeHS. Defence had not properly scoped and budgeted for system deployment and business implementation, including: changes to Defence's core ICT systems to interface with DeHS; hardware upgrades to support 1200 concurrent DeHS users; and training requirements and user software licences. While Defence expected that some 50 per cent of JHC's workforce (1200 of 2500

42 Department of Finance and Deregulation, *Gateway Review Process—Overview for the Senior Responsible Official*, November 2009. At the time, Gateway Reviews were coordinated by the Gateway Unit in the Department of Finance and Deregulation.

43 Correspondence from the Minister for Finance and Deregulation to the Minister for Defence, 20 December 2010.

JHC's workforce (1200 of 2500 staff) would access DeHS based on MoD's experience, Defence had initially purchased only 400 software licences.⁴⁴

2.32 Defence obtained approval from National Security Committee of Cabinet in February 2014 to increase the DeHS budget by a further \$47.4 million. According to Defence's submission to government, the requirements for an eHealth system had grown substantially over time, and the need to refine the scope and increase the budget reflected a better understanding of Defence's current and long term needs in managing health services for ADF personnel. The budget adjustment increased the overall cost of the project to \$133.3 million, some \$110.0 million higher than the original budget. While Defence did not request supplementary funding from government, there is nevertheless an opportunity cost associated with Defence allocating significant additional funds to deliver the project.

2.33 In summary, Defence's budgeting and approval processes for the implementation of DeHS were deficient, resulting in substantial cost increases and criticism within government.

Shaping the system to meet business requirements

2.34 On a more positive note, Defence recognised the benefits of implementing an off-the-shelf solution. According to CSC, the EMIS Primary Care System (EMIS PCS) is designed to effectively support the detailed care processes involved between the patient and primary health care providers, as well as practice management of health centres.⁴⁵ EMIS PCS has been used by the MoD for some time as an interoperable medical information and communications system. The functionality delivered by EMIS PCS to MoD is similar to Defence's business requirements for DeHS.

2.35 The DeHS design involves a number of integrated clinical modules to enable collaborative work across primary care settings and health groups. Authorised health care providers can gain access to DeHS to immediately review patient eHealth records. This removes potential delays in retrieving (paper-based) medical records, specialists' reports, diagnostic imaging and

44 The original contract with CSC included 400 user software licences, at a cost of \$4.2 million; and in August 2014, Defence paid \$4.3 million for 600 additional licences.

45 CSC, 'Response to Request for Tender', Tender Data Requirements 19, pp. 10–11.

pathology results, and provides for a better understanding of patients' medical history, prescriptions and treatments during clinical consultations.⁴⁶

2.36 Accessing patient eHealth records and summary reports from DeHS involves four steps (illustrated in Figure 2.2):

- *people*—role-based access controls distinguish between clinical practitioners, practice managers and administrative personnel;
- *access*—access to DeHS is via the Defence Restricted Network (DRN) using a Desktop PC or a 'computer-on-wheels'⁴⁷, or via a standard (public) Internet connection using a Windows-based PC with Internet Explorer;
- *ICT systems*—eHealth records are stored in the DeHS primary data centre, and other information systems that interface with DeHS can amend data, append clinical information to patient records and extract information for Defence reporting; and
- *reporting*—Defence executives, practice managers and administrative personnel receive various health reports.⁴⁸ Data that is required and approved to inform reporting is extracted from the primary data centre and stored within separate infrastructure hosted within the Defence network.⁴⁹

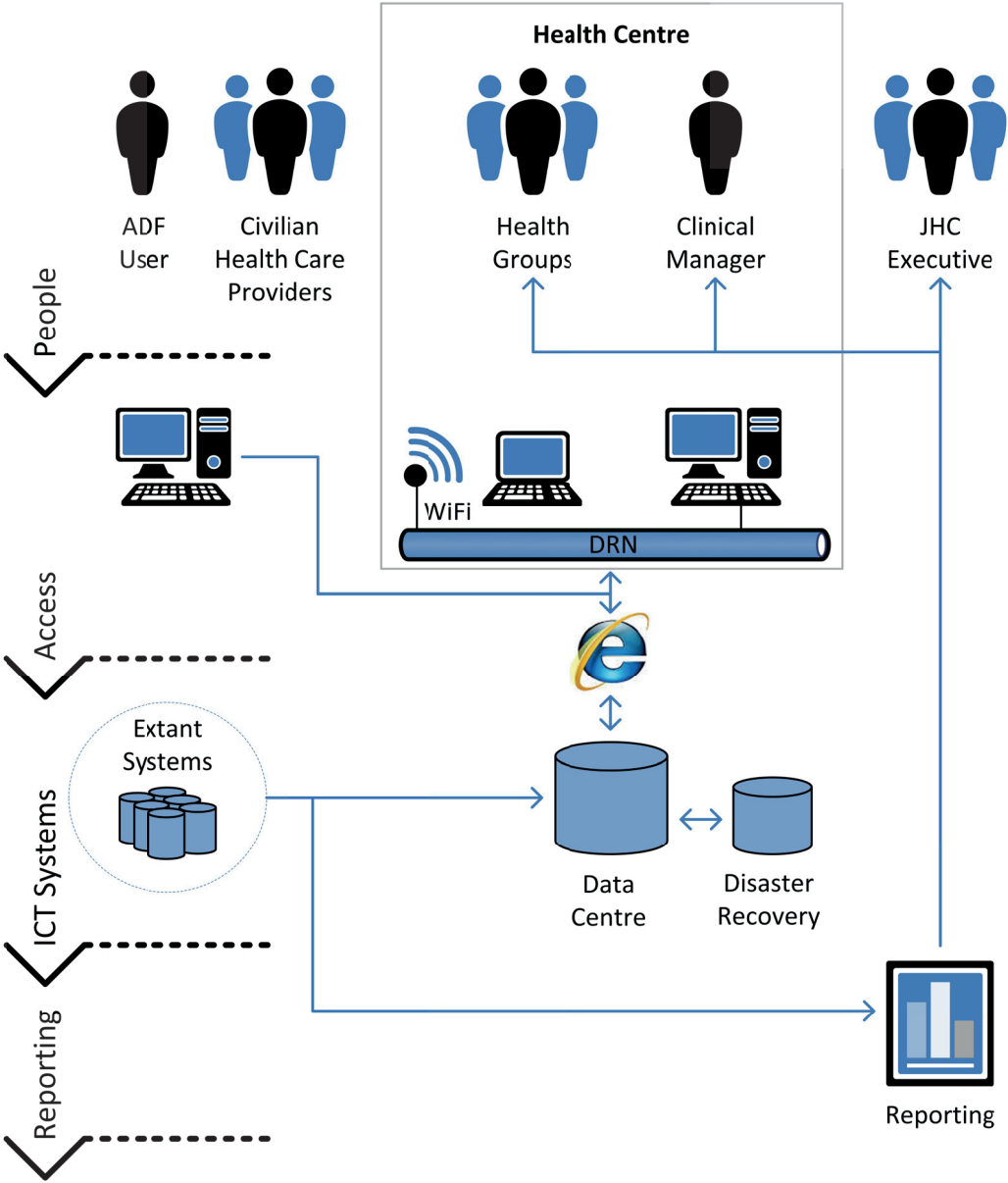
46 It is also intended that ADF personnel will have (read only) access to their own medical record to complete self-service tasks, such as confirming appointments, checking immunisation schedules and receiving clinical assessments of diagnostic imaging and pathology results.

47 That is, a wireless Internet connected laptop that is stored and secured to a (mobile) medical trolley, usually located beside a clinical ward bed—more commonly referred to as a computer-on-wheels or 'COW'.

48 Reporting may include: business intelligence and analysis per health issue, site or health region; health trends; and the deployment readiness of individuals and Force Elements.

49 Reports are produced with the assistance of a JHC Reporting Cell. This team uses Cognos to analyse requirements and extract the necessary data. Cognos is a business intelligence tool that provides reporting, analysis, dashboard and scorecard capabilities, and is in use throughout Defence. Reports are produced in various formats, including HTML, PDF and Excel, and are generally distributed via email to nominated JHC personnel.

Figure 2.2: Typical steps for accessing eHealth records from the primary data centre and developing reports



Source: ANAO analysis of DeHS processes.

2.37 The build and implementation phases of DeHS occurred in parallel with other ADF business change initiatives, as part of a broader JHC transformation. This approach required Defence to align the DeHS clinical service delivery model with JHC's new concept of operations, including:

- *an organisational restructure of JHC*—nine Area Health Services were replaced by five Regional Health Services, with five Regional Health Directors responsible for coordinating health service delivery within their region, including clinical services, resource management and training of personnel⁵⁰; and
- *realigning the health services support model, including its contractual arrangements*—in October 2012, Medibank Health Solutions (MHS) commenced administering national health care services for Defence, by providing access to medical practitioners and specialists, allied health professionals, hospital, radiology, pathology and optometry services, and referral services.⁵¹

2.38 MHS personnel administer both on-base and off-base health care services for ADF personnel. DeHS is the primary health care system for on-base services, with consultations, prescriptions and treatments directly recorded in patient Defence eHealth records. In contrast, health professionals do not use DeHS when performing off-base services because the system is only being deployed in the Garrison Health environment. DeHS is technically able to interface with MHS and there are ongoing discussions to facilitate the commencement of this process. Currently the transfer of consultation notes, specialist referral and diagnostic summary reports relies on the exchange of paper-based files.⁵²

2.39 In summary, DeHS is designed to support clinical care processes between patients and health care providers, as well as practice management of health centres and reporting on health care activities. However, DeHS is designed to interface with external health care services if the provider elects to do so.

50 Health services in each region may include: primary medical and dental care; mental health care; low dependency inpatient services; diagnostic services; allied health, including physiotherapy; medical logistic support, including pharmacy; and rehabilitation.

51 Defence health services are delivered by a multidisciplinary team of internal and external health providers, including ADF members, APS employees, civilian contractors and civilian organisations.

52 A patient file that is created as part of an off-base activity, and considered of relevance to their Defence medical record, is emailed to the regional on-base facility to be printed and scanned. The electronic copy of the file is appended to their eHealth record, and the paper-based file is then destroyed. This activity is usually completed by an Enrolled Nurse.

Conclusion

2.40 Defence's initial 2009 DeHS project proposal and budget were not properly scoped, made an incorrect assumption about ICT hosting arrangements, and were not appropriately validated prior to approval. Further, the approved budget did not include funding for progressive deployment of the system in the Garrison Health and operational environments, and the absence of costing detail in the proposal was not identified as a concern.

2.41 Defence did not seek ministerial approval of the DeHS project in 2009 in accordance with government requirements. Defence first informed the then Minister for Defence about the DeHS project in February 2010, before releasing the Request for Tender. In its advice, Defence informed the Minister that the estimated cost of the project was \$19 million when the approved cost was actually \$23.3 million, and in excess of the financial threshold for approval by the Minister for Defence.

2.42 Defence's approach to market in February 2010 differed from the DeHS business case in that it sought bids for an externally hosted system and ongoing support, rather than an internally hosted system. This change in direction had significant implications for the project's scope and budget, and contributed to a subsequent approach to government seeking approval of significantly higher project costs.

2.43 Five companies responded to the tender, each with international experience in designing, building, implementing and hosting an eHealth system. The tender evaluation team assessed the tenders against the evaluation criteria and shortlisted two companies to conduct negotiations for best and final offers. CSC was selected as the preferred tenderer on the basis that it offered a robust and proven (off-the-shelf) solution that represented value for money and reduced financial, corporate and legal risks.

2.44 In November 2010, in the context of finalising the tender selection process, Defence arranged for concurrent approval by the Minister for Defence and Finance Minister of revised DeHS project funding of \$85.9 million. A key matter raised by the Finance Minister was the conduct of an independent Gateway Review for the project, and it is not evident from Defence records why a Gateway Review was not undertaken.

2.45 In early 2012 JHC requested a Defence internal audit to address scope and cost concerns and established a program manager to take over the running of the requisite program of work. The audit found that Defence had not properly scoped and budgeted for system deployment and business implementation, including: changes to Defence's core ICT systems to interface with DeHS; hardware upgrades to support 1200 concurrent DeHS users; and user software licences and training requirements. To fund additional system components and features, Defence obtained approval from the National Security Committee of Cabinet in February 2014 to increase the DeHS budget by a further \$47.4 million.

Recommendation No.1

2.46 To provide reasonable assurance that complex ICT project proposals and cost estimates are reliable, the ANAO recommends that Defence reinforce the internal accountabilities necessary to:

- (a) properly scope, cost and validate project proposals; and
- (b) adhere to approved project management methodologies, ministerial approval and Gateway Review processes.

Defence response: *Agreed*

2.47 *Defence has already made significant improvements in the assurance of ICT projects. Since the inception of the DeHS project and the deficiencies identified within this audit, CIOG and Defence have improved governance around approval processes including:*

- *establishing the Business Relationship Management Office with dedicated personnel involved in understanding client requirements;*
- *limiting the ability to procure ICT capability outside CIOG;*
- *mandatory involvement of financial assurance staff in reviewing project approval documentation; and*
- *establishing the ICT Investment Review Committee.*

2.48 *CIOG has established professionalisation streams including:*

- *establishing a dedicated Project and Program Management stream;*
- *professionalising project and program managers;*
- *enhancing the roles of the CIOG Portfolio Management Office; and*
- *formalising structures placed around projects (including identification of Responsible Officers).*

2.49 *The professionalisation of project and program managers has reinforced the internal accountabilities necessary to adhere to approved project management methodologies, ministerial approval and Gateway Review processes.*

2.50 *Defence is confident ICT project and program management and internal accountabilities necessary to properly scope, cost and validate project proposals has improved.*

2.51 *The delegations for the procurement of ICT both software and hardware are centralised to CIOG under FINMAN 2 Schedule 1 Part 3 & 4. This excludes all groups and service ability to procure ICT without involvement of CIOG.*

2.52 *All proposals including ICT are now reviewed by embedded finance staff within VCDF under the Finance Shared Services model.*

3. System Implementation

This chapter examines Defence's project management and implementation; the security and integrity of information maintained in DeHS; and the development of standardised DeHS business processes.

Introduction

3.1 The successful implementation of an eHealth system is dependent on sound project management and implementation, including rigorous ICT system development and testing, and a consultative approach to rolling out and making improvements to the system. It is also critical that the health information captured in the system is accurate and secure so that stakeholders have confidence in the integrity of the system. The ICT component is only one part of an eHealth solution, which relies on the design and implementation of standardised business processes to achieve efficiencies in health practice and effectively capture useful information for health reporting and management purposes.

3.2 In this chapter, the ANAO examines:

- DeHS project management and implementation;
- the security and integrity of information maintained in DeHS; and
- delivery of standardised DeHS business processes.

Project management and implementation

3.3 Government entities should develop and implement complex ICT systems in accordance with endorsed program or project management methodologies.⁵³ Key success factors include close oversight of the project, and regular testing and feedback to identify and resolve ICT and business issues and meet business requirements. Defence considered the lessons learned from past attempts to deliver eHealth systems⁵⁴, which had experienced shortcomings, and decided to adopt a staged approach for the design, build, testing and implementation of DeHS.

53 The UK Office of Government Commerce (OGC) guidance *Managing Successful Programmes* (MSP) and *Prince2* are two endorsed methodologies for managing complex programs and projects.

54 HealthKeyS and MIMI were two competing and discrete Defence eHealth systems that did not meet clinical user needs or Defence's management requirements.

Summary assessment

3.4 To assess Defence’s overall effectiveness in project managing and implementing DeHS, the ANAO examined whether:

- project and ICT system roles, responsibilities and decision rights are clear, and monitored through an agreed accountability framework;
- the ICT system is: robust and reliable; secure from unauthorised access; and capable of, or expandable to, support increases in users;
- the ICT system integrates with appropriate Defence systems to support the eHealth system, and can integrate with extant information systems across Australian Government entities and health services;
- requirement, system and usability acceptance testing was conducted to deliver functional and business requirements, and optimise performance; and
- the ICT system is deployed as designed, maintained to deliver ongoing and optimal performance, and enhanced as required.

3.5 Table 3.1 provides a summary assessment of Defence’s overall effectiveness in project managing and implementing DeHS. The table shows the state observed by the ANAO as at September 2014; and the planned state as anticipated by Defence by March 2015.

Table 3.1: Summary assessment of Defence’s effectiveness in project managing and implementing DeHS

Criteria	Assessment of effectiveness			
Project manage and implement				
Establish management arrangements.				
Build ICT environment.				
Connect with extant systems.				
Gain system assurance.				
Deploy and maintain ICT system.				
KEY:	<div><div>Limited effectiveness—delivered minimal outcomes</div><div>Partially effective—delivered some of the outcomes</div><div>Generally effective—delivered most of the outcomes</div><div>Effective—delivered outcomes</div></div>			
Observed state at September 2014				
Defence's planned state by March 2015				

Source: ANAO analysis.

Establishing management arrangements

3.6 Typically, ICT project documentation provides information on proposed management arrangements, covering issues such as: decision-making and governance (*the project sponsor, governance committee or project board*); oversight and control of the project (*the steering committee*); and day-to-day management and reporting on progress, problems and review points (*the project manager*). Effective management arrangements can instil confidence in decision-makers that all stages of the project are well managed and that project status updates are timely, accurate and useful.

3.7 DeHS management arrangements were established upon project commencement in June 2009. The project governance framework set out organisational arrangements, roles and responsibilities, resources, communication arrangements, and monitoring and reporting arrangements. Two key elements of the governance framework were a DeHS Project Board and project management arrangements.

3.8 The Project Board is chaired by the Commander Joint Health and includes senior representatives from Defence's Chief Information Officer Group (CIOG), senior users within Joint Health Command (JHC), the program manager, independent advisors, and the contractor (CSC). Board Meetings have been held monthly and minutes of meetings record project status updates, discussions and key decisions made to inform project directives.⁵⁵ In the design and build phases of the project, Oakton represented the Commonwealth as the project manager and provided project management support.

3.9 There were clear signs that implementation of DeHS was off-track in 2011. Defence's Audit Branch undertook fieldwork for an internal audit focused on implementation of DeHS, in particular the adequacy of security and privacy controls. The resultant internal audit report stated that:

Audit expected that planning and project documentation to be more advanced than was observed during the review. This is particularly relevant to the security design, data migration process and benchmarking of compliance against legislation (being privacy and records management legislation). Given

55 Key activities overseen by the Board include: approving contract change proposals as submitted by CSC; managing issues and approving mitigation strategies to support the phased rollout across health centres; initiatives to improve business and technical functionality of DeHS; and adjusting performance frameworks to deliver intended outcomes. It is intended that the Project Board will continue to have an oversight role for DeHS into the sustainment phase.

the extreme reputational exposure from failure to manage security, privacy and data accuracy in connection with healthcare records, and the short time frame to implement the system (less than five months), priority must be given to address these issues.⁵⁶

3.10 Project Board minutes also recorded shortcomings in the contribution of CIOG. There were delays in the delivery of DeHS work packages by CIOG, including integration of DeHS with extant Defence information systems, and delivery of ICT hardware to Garrison health environments.

3.11 Following on from the findings of the internal audit, in October 2011, the Commander Joint Health requested that the Defence Audit Branch assess DeHS project management, implementation management and financial management. The internal audit report noted that:

Joint Health Command (JHC) formally established a related Business Implementation Team (BIT) project in April 2012. This team is responsible for managing organisational level change management (including training), the development of policies and procedures, and undertaking tasks which fall outside the scope of the [DeHS] project team. As at August 2012, the terms of reference and project plan for the BIT project had not yet been finalised.

The development and business implementation of the [DeHS] system relies on the delivery of both the [DeHS] and BIT projects. The current governance arrangements for the two projects are ineffective due to overlaps in scope, diluted accountability and unclear lines of responsibility.⁵⁷

3.12 In essence, JHC had not followed the advice of program and project management methodologies by planning and coordinating for both ICT and business changes from the outset of the project. Defence initially adopted a narrow implementation approach, focusing on delivery of the project's ICT component, rather than a broader program focus which treated DeHS as a key ICT enabler of Defence's health system and capability. JHC lacked experience in managing complex ICT-related projects, and CIOG's contribution was limited; weaknesses in internal project governance and coordination arrangements which introduced substantial additional risk.

56 Defence Audit Branch, Audit Task No.12–029, *Implementation of Joint eHealth Data—Phase 1*, October 2012, p. 5.

57 Defence Audit Branch, Audit Task No.13–046, *Implementation of Joint eHealth Data—Phase 2*, November 2012, pp. 4 and 5.

3.13 In September 2012, a program management structure was implemented to provide joint governance and oversight of ICT-related activities and business reform. The revised governance and management arrangements involved: establishing a DeHS Program and aligning system and business implementation projects; realigning the Projects Board's focus on program-related issues, the budget, risks and business implementation; assigning program management responsibility to a JHC staff member with program management support to be provided by Oakton resources; and establishing weekly meetings between JHC and CSC. Further, in late 2012, the Project Board decided to manage a range of project risks by rescheduling full DeHS implementation for late 2013—a 12 month delay in the schedule.

3.14 In April 2013, the Project Board informed the Defence Advisory Committee⁵⁸ of a number of key achievements it attributed to the new governance restructure and program management arrangements, including:

- more than 80 per cent of the procedures which align system functionality with business requirements had been finalised;
- strengthened governance and oversight of the project's financial status and funding requirements;
- reprioritisation of identified system and business enhancements;
- implementation of internal audit recommendations was nearing completion; and
- a more cohesive and coordinated approach to the rollout of DeHS.

3.15 In summary, DeHS management arrangements were inadequate through to mid-2012 because they did not provide for coordinated oversight and development of both ICT-related activities and business reform—a shortcoming which highlights that Defence did not follow endorsed program and project management methodologies. Project governance and management arrangements have improved over time, notably following internal review. The Project Board's assessments of overall progress led it to delay full implementation by 12 months so as to mitigate risk.

58 That is, the Secretary and Chief of the Defence Force Advisory Committee (SCAC).

Building the ICT environment

3.16 DeHS is complex in design and build, and the system relies on a well implemented and managed ICT environment to deliver intended functionality in a secure and timely manner.

3.17 As previously discussed, Defence recognised the benefits of implementing an off-the-shelf solution, and in January 2011 entered into a contract with CSC to procure the Primary Care System (EMIS PCS) used by the UK Ministry of Defence (MoD).⁵⁹ During the subsequent build phase of the DeHS project, CSC made necessary configuration changes to the off-the-shelf system to accommodate Defence's business needs, while retaining the integrity of the system for future upgrades. CSC also produced detailed design specifications, ICT architecture and supporting artefacts to address Defence's business requirements for system interoperability with extant information systems.

3.18 A high-level description of DeHS is one of a complex system-of-systems located across geographically dispersed ICT environments. The core of the system is the EMIS PCS suite of clinical modules that provide the user interface to capture and retrieve patient data. EMIS PCS and patient eHealth records are stored in a centralised primary data centre in Sydney. Data and health information is exchanged between DeHS and other internal and external information systems through a secure network. Only data that is required and approved to inform reporting is extracted from the primary data centre and stored in separate infrastructure hosted within the Defence network. Backup data is stored within a secondary data centre located in Melbourne, for use in the event of disaster recovery.

3.19 A user description of DeHS is one of a centralised eHealth system that is accessible by authorised users through a web interface from the Defence network or via any standard (public) Internet connection. The system is a fully managed service, including IT maintenance, server back-up and software upgrades.

⁵⁹ See paragraph 2.18.

Connecting with extant systems

3.20 A high-level functionality requirement of DeHS is the exchange of data and health information with other ICT systems located inside and outside the Defence network.

3.21 Defence relies on management information from its systems to make key decisions concerning current and future personnel and equipment availability, and to assess preparedness and operational readiness. Defence has three enterprise resource planning systems in the management information domains of:

- *personnel*—the Personnel Management Key Solution (PMKeyS);
- *finance*—the Resource and Output Management and Accounting Network (ROMAN); and
- *logistics*—the Military Integrated Logistics Information System (MILIS).

3.22 The implementation of DeHS is intended to support Defence management with a fourth enterprise-level resource planning system, in the health domain.

3.23 An interface between DeHS and PMKeyS is planned to be implemented this financial year and will support the up-to-date exchange of relevant personnel information. The data exchange reduces multiple sources of the same data and the administrative overhead when personnel records are updated.

3.24 In order for DeHS to interface with other systems, Defence needed to work with third party vendors to plan, fund and make changes to related systems. However, this scoping activity was not progressed and Defence was not well positioned to proceed with system interfaces. As a consequence, Defence decided to not enable:

- an interface to ROMAN;
- integration with Defence's extant dispensing module for pharmaceutical services (FRED) and pharmaceutical information logistic system (PILS); and
- electronic reporting (eReports) and referrals (eReferrals) from civilian health care providers' NEHTA-compliant eHealth systems.

3.25 Defence's decision not to exchange financial data between systems followed the awarding of the Garrison Health service contract to Medibank

Health Solutions (MHS), including financial reporting responsibilities. Defence also took into account the scope and cost to reconfigure ROMAN, which was considered to be approaching the end of its service. Defence now relies on MHS's accounting information system for invoicing and financial reporting on Garrison Health services.

3.26 In relation to the interface between DeHS and FRED/PILS, a July 2012 briefing from the DeHS project manager to the Commander Joint Health noted that:

The Contractor is responsible for the [DeHS] System end point of the interfaces ... The Contractor will not be responsible for the external end points of the systems for the aforementioned interfaces. ...

It should be noted that the [DeHS] project was not funded to upgrade internal Defence systems to participate in information exchange with [DeHS]. Thus funding for any external interfaces would have to be sought for what is essentially Commonwealth Furnished Material.⁶⁰

3.27 Defence's decision not to proceed with system interfaces has delayed the implementation of agreed DeHS functionality and the realisation of intended benefits, until after the system rollout. In late 2014, JHC informed the ANAO that a DeHS post-implementation plan was being drafted. The plan is to reassess the suitability, risk and cost of DeHS interfacing with other Defence systems, and other enhancements to DeHS functionality, as part of JHC's business as usual activities. To deliver intended benefits of DeHS, JHC's post-implementation plan should clearly identify resources and a timetable to implement agreed DeHS functionality.⁶¹

3.28 In terms of broader eHealth systems, Defence took into consideration the National eHealth guidelines and specifications to facilitate interoperability between civilian and ADF information systems. DeHS is built to interface with compliant ICT systems⁶² outside the Defence ICT environment in order to support the exchange of data and health information with and between other (civilian) health care providers. The National eHealth Transition Authority (NEHTA) is leading the uptake of eHealth systems of national significance and

60 Defence, Brief for Commander Joint Health, 'JeHDI Project: Interface with FRED/PILS', July 2012.

61 In December 2014, Defence informed the ANAO that functional specifications have been developed and a design document is being prepared for the introduction of a dispensing management module.

62 To exchange data between systems without transmission error, network connections must be in place and systems must mutually comply with technical specifications and business standards.

coordinating the progression and adoption of eHealth by delivering integration infrastructure and standards.⁶³ NEHTA has indicated that DeHS complies with the (provisional) standards and specifications set by NEHTA, and the system is intended to be interoperable—today and in the future—with external entities’ information systems that are NEHTA-compliant.⁶⁴

Gaining system assurance

3.29 Testing is applicable to all ICT projects and involves gaining assurance that the product and system being developed meet their specifications and work effectively. Several testing approaches are applied at different stages of design and build of an ICT system, such as testing individual parts or modules, and at the level of all parts working together as an integrated system.⁶⁵

3.30 While proven ‘off-the-shelf’ systems are expected to be generally free from defects, DeHS required configuration changes to accommodate Defence reporting needs and NEHTA standards for clinical terminology.⁶⁶ These changes required comprehensive testing to mitigate ‘new’ business and technical risks.

3.31 Testing of DeHS was conducted from September 2011 to June 2013. It included application and integration testing, user acceptance testing, system performance testing, and disaster recovery testing.

3.32 The application and integration testing focused on the technical functionality of the system to ensure EMIS PCS operates as intended, and that DeHS—as a system-of-systems—interfaces with extant Defence ICT systems and accurately exchanges data. CSC prepared 42 test cases and identified over

63 In December 2010, NEHTA set about defining standards critical to the design and development of a Personally Controlled eHealth Record (PCEHR) including standard specifications for clinical documents; Australian profiles for interoperability with PCEHR systems; a web services profile for PCEHR interoperability; guidance on representing common message content in clinical documents; and standards on core functionality and clinical presentation. In November 2011, NEHTA released a Specifications and Standards Plan. To date the NEHTA standards and specifications are not endorsed.

64 In May 2013, DeHS received provisional accreditation from NEHTA. This accreditation acknowledges that DeHS, as an eHealth records and information management system, is compliant with NEHTA standards and guidelines. It also acknowledges that the design and build of DeHS is interoperable with other NEHTA-compliant systems.

65 The types of testing include: component or unit; module; system; logical or function; volume or stress; user experience; end-to-end; configuration; usage acceptance or user acceptance; security or audit; and pilot testing.

66 A clinical terminology (CT) is a structured vocabulary used in clinical practice to accurately describe the care and treatment of patients and covers complex concepts such as diseases, operations, treatments and medicines. SNOMED CT-AU is the Australian Government endorsed clinical terminology. It was released in Australia in December 2009 and is based on the international version of SNOMED CT, but encompasses words and ideas that are clinically and technically unique to Australia.

70 issues requiring corrective action. Regression testing validated that the defects were reduced and did not exceed agreed defect limits.⁶⁷

3.33 User acceptance testing focuses on the business functionality of the system to ensure standardised business processes operate as intended in supporting day-to-day business activities. JHC invited representatives from across Defence health groups to conduct user acceptance testing over a two day period in May 2013. CSC prepared 29 test cases and identified over 30 issues requiring corrective action. Regression testing validated that the defects were reduced.

3.34 Despite comprehensive testing, issues generally emerge during pilots and system rollout that may require corrective action. This can lead to further work for the project team, including assessing identified issues and prioritising corrective actions, seeking formal approval for system changes, and scheduling code updates into the production environment. If appropriate action is not taken in a timely manner the user community may establish alternate working practices, and in the worst case may lose confidence in the system and information contained therein.

3.35 Defence conducted a Pilot of DeHS in July 2012⁶⁸, which involved participants from across Garrison Health services. The first stage of the Pilot delivered just-in-time training in the use of DeHS, which was followed by the trial and review of standardised business processes. Thirty scenarios were prepared to reflect the spectrum of patient care typically provided by ADF health care centres. Some scenarios involved patients who were posted interstate and who had forgotten their medication, and patients who arrived at sick parade then collapsed and had to be admitted to hospital. Other scenarios involved Defence service desk support, for example, calls made to resolve 'simple' issues (Level 1 support), and more complex issues requiring redirection to system resolver groups (Level 2 and 3 support).

3.36 A post-implementation report captured the lessons learned from the Pilot. The key findings included that facilitator-led training courses were informative and appropriate, and supporting technology (desktops and laptops) generally worked as intended. However, the report also highlighted

67 Regression testing is a technique used to retest earlier coding or logical errors that occurred during the initial testing phase.

68 The Pilot was conducted at HMAS Penguin in July 2012 over two days. At the time, the phased rollout of DeHS was scheduled to commence in late 2012.

concerns and made recommendations to: further align the standardised business processes with day-to-day business activities; improve the usability and prioritisation of health consultation templates; and increase the communication frequency across health groups in the lead-up to system rollout. Some health groups also expressed concern that initial clinical consultations would take longer using DeHS.

3.37 In summary, Defence conducted system testing which led to corrective action to address defects. Defence also conducted a Pilot in July 2012 of DeHS which identified a significant number of key stakeholder concerns that Defence needed to address. Taking into account the findings of the Pilot and two Defence internal audits, the Project Board decided to delay DeHS implementation by 12 months until late 2013.

Deploying and maintaining the ICT system

3.38 In April 2014, the first of the staged rollouts of DeHS commenced in Defence's Northern Queensland Health Region. Over 20 months had elapsed since the (original) Pilot, allowing key business and technical functionality to be resolved. The Project Board elected to rollout DeHS to the first three health centres as a Pilot (Pilot 1B), as part of a cautious approach intended to gauge community feedback.⁶⁹

3.39 The ANAO interviewed clinical practitioners and practice managers from two health centres some six months after site rollout, and found general acceptance of DeHS from most Defence health groups. These health groups reported the capacity to provide better patient care with access to a single patient eHealth record. For example, registered nurses and physiotherapists found the ability to review clinical consultation notes valuable when planning patient treatments, and practice managers could follow up on missed patient appointments and schedule staff rosters 12 months in advance. While training was also reported to be successful, some health groups preferred peer support activities rather than classroom sessions, which required up to three days to complete depending on the topic or health group.

69 JHC conducted a Pilot of the system in North Queensland, at HMAS Cairns, Lavarack Barracks and RAAF Townsville. The objective of the Pilot was to evaluate the: functionality of DeHS; alignment of business processes; effectiveness of training and support systems; and impact of change associated with introducing DeHS in the Garrison Health environment.

3.40 The clinical practitioners and practice managers interviewed by the ANAO indicated that DeHS had delivered most of the intended business and technical functionality to the three health centres. However, they also initially considered there were issues requiring attention, including initial system performance, delays in accessing templates and longer clinical consultation periods for several health groups. Longer consultations had been anticipated by Defence, and the Commander Joint Health had issued a directive for consultation times to be extended from 15 minutes to 30 minutes for an interim period following site rollout.

3.41 DeHS has also increased administrative workloads in some areas. For example, pharmacists are required to record patient medication and prescriptions in both the FRED/PILS systems and DeHS⁷⁰; and external health care providers are required to submit clinical reports and referrals in paper-based format for scanning, before electronic files are appended to patient eHealth records.

3.42 By September 2014, 370 registered business and technical issues identified by the DeHS user community remained unresolved. Defence and CSC advised the ANAO that they were meeting weekly to review the defects and issues log and prioritise corrective actions.⁷¹

Security and integrity of information

3.43 Health information has the greatest value when it is accurate, up to date, and accessible to the right people where and when it is needed. According to NEHTA, health information should be consistently controlled, monitored and traceable across eHealth systems to increase certainty that it is created and accessed in a secure and trustworthy manner.

70 The Project Board decided not to proceed in interfacing DeHS with FRED & PILS—the primary dispensing and stock logistic systems for pharmacists. Instead the EMIS Dispensing module is scheduled to be implemented as part of business as usual activities in late 2015.

71 Product code changes are the responsibility of Egton Medical Information Systems (EMIS) in the UK, with regression testing performed by CSC using its Adelaide testing facilities. System configuration changes are generally released into the production environment within days-to-weeks, while more complex code changes are released in three-to-six monthly intervals.








Summary assessment

3.44 To assess Defence's overall effectiveness in protecting the security and integrity of information maintained in DeHS, the ANAO examined whether:

- patient records were migrated from extant information systems—including data from paper and electronic files—to inform the eHealth records;
- a single patient eHealth record is captured, stored and accessible to authorised health services; and
- patient eHealth records are secure and ICT security controls are in place to:
 - grant only authorised personnel access to append information to and change patient eHealth records;
 - establish uniquely identifiable user accounts; and
 - capture and maintain complete audit logs as a basis for reviewing unauthorised and inappropriate activities.

3.45 Table 3.2 provides a summary assessment of Defence's overall effectiveness in protecting the security and integrity of information maintained in DeHS. The table shows the state observed by the ANAO as at September 2014; and the planned state as anticipated by Defence by March 2015.

Table 3.2: Summary assessment of Defence's effectiveness in protecting the security and integrity of information maintained in DeHS

Criteria	Assessment of effectiveness			
Security and integrity of information				
Migrate data from extant systems.				
Consolidate data into a single record.				
Maintain and review data security and integrity.				
<div><div><div>Observed state at September 2014</div><div>Defence's planned state by March 2015</div></div><div><div>Limited effectiveness—delivered minimal outcomes</div><div>Partially effective—delivered some of the outcomes</div><div>Generally effective—delivered most of the outcomes</div><div>Effective—delivered outcomes</div></div></div>				

Source: ANAO analysis.

Migrating data from extant systems

3.46 Moving data from one ICT system to another is generally an automated process of extracting and converting existing data into a new required format while preserving the integrity of the data. Large-scale data conversions across multiple systems can potentially become a project-within-a-project since considerable analysis, design and planning is generally required.

3.47 Defence's original business requirement was to rationalise and consolidate ADF health records available in extant Defence ICT systems (HealthKeyS and MIMI) to inform DeHS. At the time of the DeHS business case, Defence knew that extant eHealth information on ADF personnel was incomplete. The degree of accuracy of the eHealth records was not known.

3.48 CSC designed and built interfaces between systems to support data migration, and tested the data migration process to a Defence approved Data Migration Plan. However, after examination of the extant systems it became apparent that there were problems with the quality of the data to be transferred into the DeHS. The Project Board decided not to proceed with the migration of poor quality data. In its place the Board directed the preparation of basic health summaries from patient Unit Medical Records.⁷² While this is a not an optimal outcome, the Board made a pragmatic decision to reduce risks related to data conversion.

3.49 Defence advised in early March 2015 that to maintain access to relevant information and data from the legacy systems, JHC and Defence Support and Reform Group have agreed a set of principles for the analysis and migration of decommissioned system data, to be added to a medical records file in the Defence records management system, known as Objective. This process is intended to ensure that the legacy data is accessible in digital form from a single location to clinicians. On this basis, Defence considers that the planned state for migrating data from extant systems will be more advanced than originally anticipated and reported in Table 3.2.⁷³

72 A Health Summary for each patient includes health information such as allergies, blood type and immunisation history. Base Data Capture is the activity that transcribes a patient Health Summary from Unit Medical Records to DeHS.

73 The planned state summarised in Table 3.2 reflected Defence's expectations by March 2015.

Consolidating data into a single record

3.50 DeHS is Defence's primary system for current patient health information but it is not the only repository for patient medical records for many ADF personnel. This is due to the shortfall in migrating health information from extant Defence systems (paper and electronic) and the deferral of the implementation of the pharmaceutical dispensing module until late 2015.

3.51 For recruits joining the ADF in 2016, DeHS may be the only system that will manage their entire patient record—from recruitment to discharge—while the medical history of current ADF members may need to be accessed from multiple sources, as required.

3.52 Clinical practitioners have reported that clinical care of patients is generally not compromised by the absence of a complete patient medical history in DeHS, and that on occasions they will revert to Unit Medical Records to inform a patient's treatment strategy. However, certain health groups have been inconvenienced by the absence of records, such as dentists recording details of patients' dental history following the rollout of DeHS.

3.53 DeHS is also intended to support patient administration activities. Clinical practice managers have consolidated views of clinicians' appointments and follow-up reminders for patient reports; and patients receive forthcoming appointment notifications via SMS or email messages.⁷⁴ However, health care providers that do not have access to DeHS must submit specialists' reports and patient referrals via paper or fax to be scanned and appended into the patient eHealth record in DeHS.

Maintaining and reviewing data security and integrity

3.54 The protection of Australian Government systems and information from unauthorised access and use is a key responsibility of entities, having regard to their business operations and specific risks.⁷⁵ Preserving the confidentiality,

⁷⁴ Although potentially useful, ADF members that nominate to receive an SMS about consultations receive a basic message stating the appointment date and consultation time. The text message does not identify the clinician or health service the appointment refers to, nor provide location details. In the event an ADF member has scheduled several appointments for a day, multiple text messages are received without distinguishing between the appointments. ADF members are left with little option than to contact their Garrison Health centre to obtain more information, placing additional administrative duties on the ADF member and health centre staff.

⁷⁵ ANAO Audit Report No.50 2013–2014, *Cyber Attacks: Securing Agencies' ICT Systems*, p. 35.

integrity and availability of data and information is central to information security. According to the *Protective Security Policy Framework* (PSPF)⁷⁶: *confidentiality* ensures that information is accessible only to those authorised to have access; *integrity* ensures the safeguarding, accuracy and completeness of information and processing methods; and *availability* ensures that authorised users have access to information and associated assets when required.

3.55 A core function of DeHS is maintaining the confidentiality, integrity and availability of patient health information. The design and build of DeHS is accredited⁷⁷ to relevant security standards, and maintenance arrangements for the system are designed to comply with the *Australian Government Information Security Manual* (ISM) for physical security of the system and IT general controls that deal with system risks.⁷⁸

3.56 Access to eHealth records in DeHS is designed to be on a 'need to know' basis. For example:

- *administrative personnel* have access to the registration and appointments functionality;
- *practice managers* have access to all administrative functions, and can configure items such as appointment books and system audit capabilities; and
- *clinical practitioners* have access to all administrative functions as well as consultation and patient eHealth records.

3.57 Role-based access controls further distinguish between health care providers that are authorised to administer already prescribed treatments from

76 The Attorney-General's Department (AGD) is responsible for administering the Australian Government's protective security policy, which has as its objective to promote the most effective and efficient ways to secure the continued delivery of government business. AGD's PSPF outlines the core requirements for the effective use of protective security as a business enabler and to facilitate government working confidently and securely.

77 In May 2013, NEHTA issued provisional accreditation of DeHS. Further, CSC's primary data centre has undergone an Australian Security Intelligence Organisation (ASIO) assessment that certifies that the physical security of the building is in accordance with the requirements of the PSPF for the storage, handling and processing of Non-National Security Classified Material up to and including the level of PROTECTED. This assessment is issued by the ASIO-T4 Protective Security Team—the primary body with the responsibility to provide protective security advice to Ministers, authorities of the Australian Government and other persons determined by the Attorney-General.

78 IT general controls (ITGC) are the policies and procedures developed to deal with an entity's identified system risks. They include controls over ICT governance, ICT infrastructure, security and access to operating systems and databases, application acquisition and development, and program change procedures. Effective implementation of ITGCs provides a level of assurance that an entity's systems are protected from ICT security threats.

those that actually prescribe treatment. For example, Registered Nurses have access to patient records for review and appending clinical notes, while Dental Assistants have their access restricted to selected files within patient records.

3.58 All information in patient eHealth records is generally filed under the clinical practitioners' default confidentiality policy, which enables other practitioners to see the information. However, a professional decision can be made on a case-by-case basis to file the information in a manner that restricts access, under another confidentiality policy. For example, a psychologist may restrict access to his or her clinical notes due to the sensitivity of diagnosis and treatment; thereby denying colleagues access to these files. In urgent medical situations, clinical practitioners have rights under the appropriate security profile to override a confidentiality policy to see the restricted information.⁷⁹

3.59 Audit logs capture data as to when eHealth records were accessed, what amendments were made, and by whom. While these logs facilitate monitoring and accountability, Defence did not have arrangements in place to periodically identify unauthorised user activity. Consistent with standards generally expected, there would be merit in Defence reviewing audit logs and identifying any unauthorised access and inappropriate data entry to eHealth records.

Standardisation of eHealth processes

3.60 Engaging key stakeholders and consulting broadly with the user community facilitates the design of effective business processes. Embedding agreed and standardised processes as business as usual practices requires good communication, commitment and responsiveness to identified issues.

3.61 For JHC, the challenges faced in defining standardised business processes for DeHS included consulting with a large and geographically dispersed stakeholder group, and reviewing many disparate workflows and health processes across Defence health groups. JHC also has to remain sensitive to clinical practitioners' preferred consultation practices.

⁷⁹ Defence informed the ANAO that health care providers receive training on confidentiality policies, and the underpinning security controls and handling procedures. Further, providers are made aware that overrides of confidentiality policies will be logged and investigated by the Regional Health Director to show just cause.

Summary assessment

3.62 To assess Defence’s overall effectiveness in delivering standardised business processes for DeHS, the ANAO examined whether:

- health groups were consulted, to help understand and analyse extant business processes, and feedback was sought from health groups to inform the proposed standardised business processes;
- effective training and support activities are in place to explain the standardised DeHS business processes, and instructions are made available on the correct use of DeHS; and
- identified issues and potential enhancements to the business processes or to the ICT system are captured, assessed, prioritised and addressed in a timely manner.

3.63 Table 3.3 provides a summary assessment of Defence’s overall effectiveness in delivering standardised DeHS business processes. The table shows the state observed by the ANAO as at September 2014; and the planned state as anticipated by Defence by March 2015.

Table 3.3: Summary assessment of Defence’s effectiveness in delivering standardised DeHS business processes

Criteria	Assessment of effectiveness
Deliver standardised business processes	
Assess extant processes to inform standardised business processes.	
Explain the standardised business processes and ICT system.	
Identify and address shortfalls, and make changes to better the system.	
KEY: <div>Limited effectiveness—delivered minimal outcomes </div> <div>Partially effective—delivered some of the outcomes </div> <div>Generally effective—delivered most of the outcomes </div> <div>Effective—delivered outcomes </div> <div> Observed state at September 2014</div> <div> Defence's planned state by March 2015</div>	

Source: ANAO analysis.

Assessing extant processes to inform standardised business processes

3.64 From the outset of the DeHS project, Defence understood the importance of rationalising and consolidating business processes to deliver planned requirements and intended outcomes. JHC had identified that business

processes were not uniform across health centres, and staff movements and deployments to different centres highlighted these discrepancies in business and workplace practices. JHC considered that the use of standardised business processes by all health groups within the Garrison Health environment would better support Defence's clinical service delivery model.

3.65 In developing the DeHS business case in 2008–09, Defence formulated an initial business process model for DeHS. The model was based on 26 separate business scenarios that addressed clinical care, practice management and reporting requirements.⁸⁰ The scenarios were not envisaged to be an exhaustive listing of all scenarios that fall under Defence health services but rather a representative list of Defence health clinical pathways.

3.66 In 2011, workshops were conducted with each health group to understand preferred business practices and validate the initial business process model. It became evident that many clinical practitioners had their own preferred business practices.

3.67 Further refinement of the proposed standardised business processes took place based on feedback from the DeHS UAT and Pilots. The feedback again highlighted shortfalls in accommodating preferred business processes. For example, DeHS generally restricts clinical practitioners to document consult notes in a set clinical sequence⁸¹; the system cannot efficiently process assessments for large number of personnel such as pre-deployment checks⁸²; and it does not permit the drafting of a patient referral letter until after the consultation notes are completed.

Explaining the standardised business processes and ICT system

3.68 Having designed, built and tested a system to required business and technical specifications, the system needs to be put to use. This is usually treated as a distinct project phase covering activities such as: organisational change management across the enterprise; training for those who will use the

80 Appendix 3 outlines the 26 business scenarios used to assess the functionality of DeHS.

81 Templates and onscreen questions (text fields) are generally completed in a set sequence before the user is permitted to progress further through the consultation notes.

82 Assessing operational readiness of individuals and Force Elements is a core function for JHC. Pre-deployment checks are conducted at three months, 40 days and five days from deployment. Clinical practitioners may be called upon to assess over 120 ADF members on a given day. DeHS cannot efficiently accommodate this workflow and paper-based records are required to be captured and later transcribed against patient records.

system in their work; publicity or communication to those who will be affected by the system; and monitoring and responding to difficulties during system implementation.

3.69 JHC designed and prepared a blended training solution of eLearning (online) modules, face-to-face and peer support activities to support the rollout of DeHS across health centres. Further, JHC developed aide-mémoires and fact sheets directed at each of the health groups, and posters for health centres to inform patients about DeHS. Site rollout of DeHS was also supported by a variety of other communications, including readiness surveys, newsletters, site visits and presentations by JHC Executives.

3.70 Defence informed the ANAO that in the initial weeks following rollout, the Commander Joint Health made weekly phone calls to Health Centre Managers seeking staff feedback on the functionality of DeHS to meet local business needs, and that Health Centre Managers were well positioned to gauge and respond to staff concerns. Defence further informed the ANAO that issues raised by staff were generally addressed within the first or second week after site rollout.

3.71 In most cases health group professionals that met with the ANAO accepted the consolidation of the extant business processes into standardised business processes—to be used by all practitioners and support staff within health groups across Garrison Health services.⁸³ However, following site rollout, pockets of clinical practitioners elected to revert to prior business practices. For example, some practitioners did not use system templates or SNOMED codes⁸⁴, preferring free text annotations in consult notes, and created workarounds to clinical steps and procedures. While alternate business practices may not compromise patient health care, the adoption of past practices does not provide a uniform basis for accurate reporting of clinical and health trends—an aid to the efficient delivery of health care services.

3.72 JHC was aware of these emerging cultural change issues. At the time of the audit, a revised JHC communication campaign was in the planning stage, and was intended to reinforce the benefits of standardised business processes.

83 In August 2014, the ANAO interviewed clinical practitioners, practice managers and administrative personnel from health centres in Lavarack Barracks and RAAF Townsville, Northern Queensland. These health centres were selected because they were the first sites to rollout DeHS and have used the system since April 2014.

84 See footnote 66.

Identifying and addressing shortfalls, and making changes to better the system

3.73 A sound risk management approach includes a willingness to act upon issues as they arise, including the unexpected. Swift, and on occasions, significant action may be needed if implementation risks begin to materialise.

3.74 DeHS is not without coding defects and system faults. It is a complex system that requires ongoing management to avoid risks to business processes and technical functionality. Mindful of user community feedback and issues identified following site rollout, JHC systematically logged and sought to address shortfalls in business and technical functionality after they were identified. Nonetheless, the process to instigate corrective action has often been slow. This is in part due to the complexity of coding and configuring approved changes in the production system. However, it is mostly due to the volume of changes required, competing operational priorities, and limited business and technical resources. Of particular note, delays can be attributed to the call on key resources during the rollout of DeHS across 64 health sites from April 2014 to late 2014.

3.75 Clinical practitioners and practice managers interviewed by the ANAO were generally accepting of DeHS with its current limitations, identified defects and emerging issues on initial system rollout. However, some health professionals expressed concern that delays in resolving defects, while currently tolerable, may undermine confidence in the system and its effective use. Some health professionals were also concerned that outstanding issues and proposed business improvements may not be resolved and implemented. In these circumstances, there is benefit in maintaining an ongoing focus on stakeholder consultation as well as remediation.

3.76 By December 2014, following the rollout of DeHS across Defence's Garrison Health environments, JHC planned to finalise surveys of stakeholder experience for each site. Timely evaluation of the survey data, stakeholders' use of the system, and system performance and issues, would help generate confidence amongst users that Defence is actively pursuing benefits realisation. It would also assist Defence to prioritise future remediation and enhancement activities for DeHS, and supplement support activities for users.

Conclusion

3.77 At the outset of the DeHS project, Defence did not follow an approved program or project management methodology, even though Defence ICT

projects are required to apply proven methodologies. In 2012, two Defence internal audits reported major shortfalls in DeHS project management, controls, reporting and documentation. Internal audit confirmed that key assumptions underpinning the DeHS business case were not valid and without greater focus on business implementation, the project would be at risk.

3.78 Defence underestimated the broader program and governance challenges inherent in the project, and did not mitigate key risks until mid-2012. Defence initially adopted a narrow implementation approach, focusing on delivery of the project's ICT component, rather than a broader program focus which treated DeHS as a key ICT enabler of Defence's health system and capability. In April 2012, nearly three years into the project, JHC assigned responsibility for DeHS organisational level change management to a newly formed team within JHC; and in September 2012, a program management structure was implemented to provide for joint governance oversight of ICT activities and business reform.

3.79 DeHS is an off-the-shelf solution. While Defence made necessary configuration changes to the off-the-shelf system to accommodate business needs, Defence retained the integrity of the system for future upgrades. Defence also intended that the system would automatically capture civilian health care provider referrals and reporting; support dispensing of pharmaceuticals; and exchange information with Defence's financial management and accounting system. However, this work was not progressed, which has delayed the implementation of agreed DeHS functionality and the realisation of intended benefits.

3.80 ANAO interviews indicate that there is general acceptance of DeHS from most Defence health groups. These health groups reported better patient care with access to a single patient eHealth record. However, stakeholders also considered there were issues requiring attention, including initial system performance, delays in accessing templates and longer clinical consultation periods for health groups.

3.81 In consultation with health groups, JHC developed standardised business processes for the use of DeHS to support Defence's clinical service delivery model. However, pockets of clinical practitioners elected to revert to prior business practices. The adoption of past practices does not provide a uniform basis for accurate reporting of clinical and health trends—an aid to the efficient delivery of health care services. Successful implementation will rely on cultural acceptance and behaviour change, and Defence should maintain an ongoing focus on stakeholder consultation as well as remediation to help realise intended benefits of the system.

Recommendation No.2

3.82 To achieve benefits realisation, the ANAO recommends that Defence:

- (a) evaluate stakeholders' use of DeHS and reinforce standardised business processes; and
- (b) finalise post-implementation planning, including by identifying resources and a timetable to implement agreed DeHS functionality.

Defence response: *Agreed.*

3.83 *To evaluate stakeholders' use of DeHS and reinforce standardised business processes JHC has established the Health Information Systems Directorate who are responsible for:*

- *building the sustainment model for DeHS;*
- *delivering reports to support standardisation of business processes and inform training and communications;*
- *stakeholder liaison to ensure the voice of the user is considered and feeds into the continuous improvement process;*
- *stakeholder engagement regarding DeHS enhancement and release management processes; and*
- *providing a business support team to manage the day to day interaction and problem rectification for users.*

3.84 *To support the standardisation of processes JHC has developed a number of Garrison Health Operations Business Processes. The finalisation of post implementation planning including resources and a Strategic Plan to embed the JHC DeHS and health information capability is well underway and include:*

- *the establishment of a Directorate responsible for Health Information Systems;*
- *development of a Health Information Management Framework;*
- *development of a Health Information Management Strategic Plan 2015–2017 incorporating the review and alignment of agreed functions in DeHS; and development of a supporting suite of activities to realise the Strategic Plan.*



Ian McPhee
Auditor-General

Canberra ACT
10 March 2015

Appendices

Appendix 1: Entity Response



Australian Government

Department of Defence

GEO
5 MAR 2015
8.50

Mr Dennis Richardson
Secretary

Air Chief Marshal Mark Binskin, AC
Chief of the Defence Force

SEC/OUT/2015/38
CDF/OUT/2015/250

Dr Tom Ioannou *78 s/3*
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2600

Tom
Dear Dr Ioannou

Australian National Audit Office Performance Audit of Electronic Health Records for Defence Personnel

Thank you for the opportunity to provide comment on the Proposed Report provided to Defence on 4 February 2015.

Defence's comments and suggested editorial amendments are included at Enclosure 1. The response to requests for information are included at Enclosure 2. The Defence response to the proposed report is included at Enclosure 3, for inclusion in the published report. Enclosure 4 sets out our response to the recommendations included in the proposed report.

Should you have any queries, please contact Mr Geoffrey Brown, Chief Audit Executive.

Yours sincerely

Dennis
Dennis Richardson
Secretary

4 March 2015

M. D. Binskin
M. D. BINSKIN, AC
Air Chief Marshal
Chief of the Defence Force

3 March 2015

Appendix 2: Summary assessment of Defence's overall effectiveness in delivering the eHealth system—status in 2014–15

Criteria	Assessment of effectiveness
Define business requirements	
Assess business requirements.	
Adopt a proven system.	
Scope, budget and procure	
Supply business requirement.	
Budget and approval.	
Shape the system to meet business requirements.	
Project manage and implement	
Establish management arrangements.	
Build ICT environment.	
Connect with extant systems.	
Gain system assurance.	
Deploy and maintain ICT system.	
Security and integrity of information	
Migrate data from extant systems.	
Consolidate data into a single record.	
Maintain and review data security and integrity.	
Deliver standardised business processes	
Assess extant processes to inform standardised business processes.	
Explain the standardised business processes and ICT system.	
Identify and address shortfalls, and make changes to better the system.	
KEY: <div> Observed state at September 2014 Defence's planned state by March 2015 </div> <div> Limited effectiveness—delivered minimal outcomes Partially effective—delivered some of the outcomes Generally effective—delivered most of the outcomes Effective—delivered outcomes </div>	

Source: ANAO.

Appendix 3: Business scenarios used to assess the functionality of DeHS

1. An outcome of the Rapid Prototyping, Development and Evaluation (RPDE) Proof of Concept was an initial business and operational process model of DeHS. During the build and testing phase of DeHS, the following 26 business scenarios were assessed as representing, as a minimum, the required functionality of the system in supporting clinical care, practice management and reporting.
2. The scenarios were not envisaged to be an exhaustive listing of all scenarios that fall under Defence health services but representative of Defence health clinical pathways.

Table A.1: Business scenarios used to assess the functionality of DeHS in supporting clinical care, practice management and reporting

Business scenario	High-level summary description of each scenario
1. Individual health record access.	An ADF member accesses his or her summary or complete health record in electronic form.
2. Annual health assessment (AHA).	A primary health care team accesses and records the information required to complete an AHA.
3. Comprehensive preventative health examination (CPHE).	A primary health care team accesses and records the information required to complete a CPHE.
4. Standard primary medical care consultation.	A general practitioner, nurse or medic accesses and records the information needed to diagnose a condition and determine a treatment.
5. Primary medical care clinical procedure.	A general practitioner, nurse or medic accesses and records the information related to the conduct and outcome of a clinical procedure.
6. Short-term primary care observation.	A nurse or medic accesses and records the information needed to observe and monitor a patient for a period of up to eight hours.
7. Primary dental care examination.	A dental practitioner, dental technician or dental hygienist accesses and records the information needed to conduct a dental examination.
8. Primary dental care procedure.	A dental practitioner, dental technician or dental hygienist accesses and records the information needed to conduct a dental procedure.
9. Physiotherapist consultation.	A physiotherapist accesses and records the information required to conduct an examination and treatment.

Business scenario	High-level summary description of each scenario
10. Clinical psychologist consultation.	A clinical psychologist accesses and records the information required to conduct a mental health consultation.
11. Primary care prescription.	A general practitioner and a pharmacist access and record the information required to prescribe and dispense a controlled medication.
12. Primary care diagnostic referral.	A primary medical or dental practitioner accesses and records the information required to order a pathology test or medical image.
13. Primary care specialist referral.	A primary medical or dental practitioner accesses and records the information required to refer a patient for specialist review.
14. Primary care non-elective hospital administration referral.	A general practitioner accesses and records the information required to refer a patient to hospital for administration.
15. Diagnostic reporting.	A primary care medical practitioner, dental practitioner, nurse or allied health practitioner accesses and records the information he or she needs to interpret and act on an imaging and pathology report.
16. Specialist reporting.	A primary care medical practitioner, dental practitioner, nurse or allied health practitioner accesses and records the information he or she needs to interpret and act on a specialist report.
17. Summary hospital discharge reporting.	A general practitioner or nurse accesses and records the information he or she needs to interpret and act on a hospital discharge summary.
18. Primary care practice management.	A primary care practice manager accesses and records the information required to schedule appointments, allocate staff resources and manage internal practice workflow.
19. Epidemiological and health surveillance reporting.	A health services staff officer accesses the aggregated information required to identify illness and injury patterns in a specific ADF population.
20. Notifiable disease reporting.	A primary medical or dental practitioner accesses and records the information required to report a notifiable disease to State and Commonwealth health authorities.
21. Financial and resource utilisation reporting.	A health service manager at practice, base, regional, command or national levels accesses financial and resource utilisation data to support management decision-making.
22. Aggregated force readiness assessment.	A staff officer in a command headquarters accesses non Medical-in-Confidence information on the individual and collective health readiness of Force Elements.

Business scenario	High-level summary description of each scenario
23. Medical employment classification (MEC) review.	A general practitioner accesses and records the information he or she needs to review the medical status of an ADF member to determine his or her deployability status.
24. Case management.	A case manager accesses and records the information he or she needs to coordinate the care of an ADF member who is receiving health services from a range of on-base and off-base health providers.
25. Health help desk enquiry and response (1800 IM SICK).	A Defence clinician accesses and records the information he or she requires to provide advice to an ADF member who calls the 1800 IM SICK help line.
26. Primary care pharmacist consultation.	A pharmacist accesses and records the information he or she needs to assess and provide medications or devices to ADF members who come to a central dispensing point as their first point of contact with the primary care health centre.

Source: Defence. All defined DeHS functional performance specifications (FPS) can be related to at least one or more business scenarios; however, the scenarios do not represent all operational situations in which the functional requirements will be utilised.

Index

A

Auditor-General, 28

Australian Government Information
Security Manual (ISM), 70

C

Chief Information Officer Group
(CIOG), 39, 57–58

Chief of the Defence Force (CDF), 26,
42–44

Commander Joint Health, 40, 44, 57, 58,
62, 66, 74

CSC Australia Pty Ltd (CSC), 25–28,
43–48, 52, 57–70

D

Defence Audit Branch, 33, 57, 58

Defence Health Groups, 25, 39–40, 48,
64–76

administrative personnel, 49, 70, 74

clinical practitioners, 49, 69–76

dentists, 25, 69

pharmacists, 66

physiotherapists, 65

practice managers, 49, 65, 66, 69–70,
75

psychologists, 71, 84

registered nurses, 65, 71

Defence Management Systems
Improvement (JP2080), 31

Department of Finance, 27, 46–47

Department of Veterans' Affairs, 29, 39

Deployable Health Capability (JP2060),
31, 46

E

Egton Medical Information Systems
(EMIS), 25, 44, 66

G

Garrison Health

environment, 26, 39, 40, 46, 51, 65,
73, 75

services, 51, 62, 64, 69, 74

Gateway Review, 47, 52–53

H

Health Key Solution (HealthKeyS), 32,
38, 41, 55, 68

J

Joint Health Command (JHC), 26, 34,
39–43, 47–53, 57–65, 71–76

M

Medibank Health Solutions (MHS), 40,
51, 62

Military Integrated Logistics
Information System (MILIS), 61

MIMI, 38, 55, 68

Minister for Defence, 26, 27, 40, 46, 47,
52

Minister for Finance, 26, 27, 46, 47, 52

N

National eHealth Strategy, 31, 39

National eHealth Transition Authority
(NEHTA), 31, 39, 43, 61–63, 66, 70

National Security Committee of
Cabinet, 27, 48, 53

O

Oakton, 25, 47, 57, 59

P

Personally Controlled Electronic Health
Record (PCEHR), 31, 32, 63

Personnel Management Key Solution
(PMKeyS), 41, 61

Primary Care System (EMIS PCS), 26,
44, 48, 60, 63

Project Board, 57–59, 65–68

Protective Security Policy Framework
(PSPF), 70

R

Rapid Prototyping, Development and
Evaluation (RPDE), 41

Resource and Output Management
and Accounting Network
(ROMAN), 41, 61, 62

S

Secretary and Chief of the Defence
Force Advisory Committee (SCAC),
59

Secretary of Defence, 26, 42–44

Strategic Reform Program (SRP), 46

T

Treasurer, 28

Series Titles

ANAO Report No.1 2014–15

Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2013 Compliance)
Across Agencies

ANAO Report No.2 2014–15

Food Security in Remote Indigenous Communities
Department of the Prime Minister and Cabinet

ANAO Report No.3 2014–15

Fraud Control Arrangements
Across Entities

ANAO Report No.4 2014–15

Second Follow-up Audit into the Australian Electoral Commission's Preparation for and Conduct of Federal Elections
Australian Electoral Commission

ANAO Report No.5 2014–15

Annual Compliance Arrangements with Large Corporate Taxpayers
Australian Taxation Office

ANAO Report No.6 2014–15

Business Continuity Management
Across Entities

ANAO Report No.7 2014–15

Administration of Contact Centres
Australian Taxation Office

ANAO Report No.8 2014–15

Implementation of Audit Recommendations
Department of Health

ANAO Report No.9 2014–15

The Design and Conduct of the Third and Fourth Funding Rounds of the Regional Development Australia Fund

Department of Infrastructure and Regional Development

ANAO Report No.10 2014–15

Administration of the Biodiversity Fund Program

Department of the Environment

ANAO Report No.11 2014–15

The Award of Grants under the Clean Technology Program

Department of Industry

ANAO Report No.12 2014–15

Diagnostic Imaging Reforms

Department of Health

ANAO Report No.13 2014–15

Management of the Cape Class Patrol Boat Program

Australian Customs and Border Protection Service

ANAO Report No.14 2014–15

2013–14 Major Projects Report

Defence Materiel Organisation

ANAO Report No.15 2014–15

Administration of the Export Market Development Grants Scheme

Australian Trade Commission

Audit Report No.16 2014–15

Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2014

Across Entities

ANAO Report No.17 2014–15

Recruitment and Retention of Specialist Skills for Navy

Department of Defence

ANAO Report No.18 2014–15

The Ethanol Production Grants Program

Department of Industry and Science

ANAO Report No.19 2014–15

Management of the Disposal of Specialist Military Equipment

Department of Defence

ANAO Report No.20 2014–15

Administration of the Tariff Concession System

Australian Customs and Border Protection Service

ANAO Report No.21 2014–15

Delivery of Australia's Consular Services

Department of Foreign Affairs and Trade

ANAO Report No.22 2014–15

Administration of the Indigenous Legal Assistance Programme

Attorney-General's Department

ANAO Report No.23 2014–15

Administration of the Early Years Quality Fund

Department of Education and Training

Department of Finance

Department of the Prime Minister and Cabinet

ANAO Report No.24 2014–15

Managing Assets and Contracts at Parliament House

Department of Parliamentary Services

ANAO Report No.25 2014–15

Administration of the Fifth Community Pharmacy Agreement

Department of Health

Department of Human Services

Department of Veterans' Affairs

ANAO Report No.26 2014–15

Administration of the Medical Specialist Training Program

Department of Health

ANAO Report No.27 2014–15

Electronic Health Records for Defence Personnel

ANAO Report No.27 2014–15

Electronic Health Records for Defence Personnel

Department of Defence

Better Practice Guides

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

Public Sector Financial Statements: High-quality reporting through good governance and processes	March 2015
Public Sector Audit Committees: Independent assurance and advice for Accountable Authorities	March 2015
Successful Implementation of Policy Initiatives	Oct. 2014
Public Sector Governance: Strengthening Performance through Good Governance	June 2014
Administering Regulation: Achieving the Right Balance	June 2014
Implementing Better Practice Grants Administration	Dec. 2013
Human Resource Management Information Systems: Risks and Controls	June 2013
Public Sector Internal Audit: An Investment in Assurance and Business Improvement	Sept. 2012
Public Sector Environmental Management: Reducing the Environmental Impacts of Public Sector Operations	Apr. 2012
Developing and Managing Contracts: Getting the Right Outcome, Achieving Value for Money	Feb. 2012
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities: Delivering Agreed Outcomes through an Efficient and Optimal Asset Base	Sept. 2010
Planning and Approving Projects – an Executive Perspective: Setting the Foundation for Results	June 2010
Innovation in the Public Sector: Enabling Better Performance, Driving New Directions	Dec. 2009
SAP ECC 6.0: Security and Control	June 2009
Business Continuity Management: Building Resilience in Public Sector Entities	June 2009
Developing and Managing Internal Budgets	June 2008