Australian Government
Department of Defence
Defence Science and
Technology Organisation

Archiving a Software Development Project

Peter Fisher

Command, Control, Communications and Intelligence Division
Defence Science and Technology Organisation

DSTO-GD-0739

ABSTRACT

The process of archiving Australian Government Records in the National Archives of Australia is non-trivial. Archiving a Department of Defence Software Development Project has added complexities. This document describes and illustrates the steps involved in the archiving of such a project. It also records the process and the issues to be considered, with the intention that others directed toward such a task will not need to rediscover the process and its requirements.

Published by

Command, Control, Communications and Intelligence Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 7389 5555
Fax: (08) 7389 6567

AR-015-589
April 2013

APPROVED FOR PUBLIC RELEASE

Archiving a Software Development Project

Executive Summary

In relation to a particular Software Development Project, it was discovered that there were ambiguities regarding the Intellectual Property ownership rights and software licensing rights of the software. It was decided that certain risks arising from these ambiguities would best be addressed by making it clear that the Commonwealth of Australia had placed itself in a position where it was unable to contravene even the broadest interpretation of these rights. It was decided that the best way to achieve this would be to lock the intellectual property in a place where it was preserved, but was not able to be retrieved without there being alerts generated, and official records of the retrieval. It was suggested that placing the information in the National Archives of Australia may be the best mechanism for doing this.

The aims of the work that this report discusses are to:

- determine if archiving the information does satisfy the risk management requirements;
- determine the requirements of, and the process for, archiving;
- determine the location of all copies of the information, and retrieve and/or destroy them;
- document the retrieval and certify the destruction;
- assemble the information to be archived, prepare it for archiving, and archive it;
- document the process and place the evidence of the successful completion of the above tasks on a registry file;
- implement an ongoing monitoring system that identifies attempts and requests for retrieval, and ensures that the attempts and requests cannot proceed without the knowledge of and authorisation from senior management.

The two major aims of recording the process were to:

- provide a record, and hence evidence, that these tasks were successfully performed, and that they were performed with due diligence, and;
- provide a record of the process that was followed and of the issues that were considered, with the intention that others directed toward such a task would not need to rediscover the process and its requirements.

This report records and discusses the process used and the related process issues.
The detailed record of the work done is captured in a report classified “commercial-in-confidence” with a very limited distribution list.

Discovering the process required involved investigation of a large amount of information, including Australian Acts of Parliament, Australian and International Standards documents, and policy and procedure manuals and guidelines. Those that proved to be relevant are summarised in the appendices of this report, as are illustrations of the information archived, and the tasks performed.

Author

Peter Fisher
Command, Control, Communications and Intelligence Division

Peter Fisher has worked as a consultant, systems analyst, software developer and project manager in Australia, Holland, the USA, England, France and Mexico. He has also worked as a Manager of Computer Operations and Support, and as a University Lecturer in Computer Science.

Peter joined the then Software Engineering Group of DSTO's Information Technology Division in 1994 and worked as a consultant to Defence projects on software engineering and software procurement matters. In 1997 he was appointed Deputy Head of the DSTO Year 2000 Project, and in 2000 he moved into the field of Information Operations research.

In 2004 he joined the executive of Command and Control Division where he investigated the "Science of C2", C2 Concepts and C2 experimentation. As Deputy Head of the DSTO Experimentation Initiative, he managed a study for improving support to the Needs Phase of the Capability Development process. He also coordinated DSTO's S&T support to the HQJOC transition to Bungendore, and worked on a mutlidiscipline crossdivisional team investigating Situation Awareness in Multi-Agency emergency management environments.

In 2009 he moved to research into providing automated and semi-automated support to Intelligence Analysts, in order to facilitate their analysis and their information management, particularly in the area of production of strategic estimates.

Peter's research interests are in the way people acquire, use and communicate information, and their information requirements to achieve their goals.

Contents

This page is intentionally blank

Glossary

24Labs	The location of the Archives at DSTO-E
40Labs	The location of the Registry at DSTO-E
AGLS	Australian Government Locator Service
Archives Act	An Act relating to the preservation and use of archival resources, and for related purposes. See 2 The Archives Act 1983 (pg 3)
AS	Australian Standard See H.3.1 National and international standards (pg 23)
AS 4390	The Australian standard for records management
AS 5090	Work Process Analysis for Recordkeeping
AS 5044	AGLS metadata standard
AS ISO 15489	The Australian and international standard for records management
BIS	Business Information Systems software guidelines See: J.1 Digital Recordkeeping: Guidelines (pg 33)
C3ID	DSTO's Command, Control, Communication and Intelligence Division
CC3ID	Chief of C3ID
CD	Compact Disk – a form of optical storage media See: http://en.wikipedia.org/wiki/Compact_Disc)
Collection	The Collection of the NAA See H.1 The Collection (pg 21)
Crimes Act	Crimes Act 1914 See http://en.wikipedia.org/wiki/Crimes_Act_1914
CVS	A software version control system See http://en.wikipedia.org/wiki/Concurrent_Versions_System
DIRKS	Designing and Implementing Recordkeeping Systems manual See H.6 IT systems that make, keep and manage records (pg 26)
Disposal Authority	A document defining how long certain types of information must be kept and if and when it can be destroyed. See 3.1.4 Disposal Authority (pg 4)
DRMS	Defence Records Management System on the DRN See 3.1.3 DRMS – Defence Records Management System (pg 4)
DRN	Defence Restricted computer Network
DSA	Defence Security Authority
DSTO	Defence Science and Technology Organisation
DSTO-E	DSTO Edinburgh SA 5111
DVD	Digital Versatile Disk – a form of optical storage media See http://en.wikipedia.org/wiki/DVD
ERMS	Electronic Records Management System software guidelines See: J.1 Digital Recordkeeping: Guidelines (pg 33)
Evidence Act	The Evidence Act 1995 See H.5 Records in Evidence: The Impact of the Evidence Act (pg 26)
FAQ	Frequently Asked Questions See H.1.1 FAQs (pg 21)
FOI Act	Freedom of Information Act 1982 See http://en.wikipedia.org/wiki/Freedom_of_Information_Act_1982
gforge	DSTO host of CVS repository See https://gforge.dsto.defence.gov.au/projects/Xxxx/
git	A software version control system See http://en.wikipedia.org/wiki/Git_(software)
IA	Intelligence Analysis discipline of IPA Branch

iaw	in accordance with
IM	Information Management
IP	Intellectual Property
IPA	Intelligence Processing and Analysis Branch of C3ID
ISO	International Standards Organisation
jira	DSTO host of a software project management task tracking system See http://jira.dsto.defence.gov.au/browse/Xxxx
mango	DSTO host of SVN repository See http://mango.dsto.defence.gov.au:8080/svn/Xxxx
lime	DSTO file server
NAA	National Archives of Australia See http://www.naa.gov.au
RM	Records Management
SCIS	DSTO's Science Corporate Information Systems group
Sharepoint	Microsoft collaboration-focussed file-sharing system See http://en.wikipedia.org/wiki/Sharepoint
Subversion	A software version control system – See SVN
SVN	Subversion - A software version control system See http://en.wikipedia.org/wiki/Apache_Subversion
wrt	with respect to
Xena	XML Electronic Normalising of Archives See J.2.1 Keeping Digital Records (pg 36)
XML	eXtensible Markup Language See http://en.wikipedia.org/wiki/XML

1. Introduction

1.1 Background

In the third quarter of 2010, it was decided that the "tangible" intellectual products of a software development project were to be "archived" in a manner that would capture and preserve the intellectual property (IP), but make it and the products generally inaccessible without the "right" authority. Further, the information was to be stored in accordance with the physical and legal requirements of the National Archives of Australia (NAA), and in a manner that would record an audit trail, (and produce alarms), of any and all attempts to access it.

At that time, no DSTO employees at Edinburgh had any idea what was required to achieve these goals, nor how to achieve them. Hence the first steps involved determining the nature and scope of the requirements, and the feasibility of achieving them. It quickly became apparent that there would be many steps in determining and carrying out the requirements, and because of the legal requirements, the compilation of a comprehensive record of the tasks performed would be an essential part of the process.

Hence, the aims of recording the process included:

- To provide a record, (and hence evidence), of the work done — in order to demonstrate that the tasks were performed, and that they were performed with due diligence.
- To record the process so that the next person required to archive a DSTO Task involving software development does not need to rediscover the process and its requirements.

The first aim has been addressed in a report classified "commercial-in-confidence" with a very limited distribution list. In particular, the layout of this document is intended as a template that can be used to facilitate achievement of the first aim. The second aim is addressed by this unclassified document.

The target audience of this document includes:

- Those with management responsibility for the legal issues being addressed by the archiving task.
- Those who may wish to gain an overview of the various, technical, physical and/or legal issues involved.

1.2 The Task

After initial investigation, the requirements and the process required were determined:

1.2.1 The Requirement

Retrieve and archive all copies of the software in a manner that provides evidence that no-one is using, and no-one can use, a copy of the software sourced from DSTO.

1.2.2 Method

Archive the software, locate all copies of the software and delete/destroy them, make a record of the deletion/destruction, and implement procedures to ensure deleted and archived copies cannot be retrieved without senior management being aware of the retrieval, or the attempted retrieval, and approving it.

1.2.3 Task list

- Determine the requirements of The Archives Act 1983 (section 2, page 3)
- Determine the requirements of The archive process (sec 3, pg 3)
- Determine What we needed to do (sec 4, pg 6)
- Do it
- Document What we did (sec 5, pg 6)

1.3 Report structure

This report records the process and issues involved in the execution of the steps listed above in section 1.2.3 Task list.

It transpired that the archive process is ***not*** specified by any Act of Parliament or law; the Archives Act specifies the roles and responsibilities of the National Archives of Australia (NAA), and the process is specified in publications issued by the NAA. The Act is summarised in section 2, The Archives Act 1983 (pg.3), and relevant sections of the Act are reproduced in Appendix L: Archives Act 1983 (pg.40). The many issues to be considered and steps to be performed when performing the process are listed and discussed in section 3, The archive process (pg.3). The relevant details and supporting explanations are reproduced in the appendices:

Appendix H: National Archives Website (pg.21)
Appendix I: Physical Records (pg.29)
Appendix J: Digital Records (pg.33)
Appendix K: GDA25 – General Disposal Authority (pg.37)

Having determined the process and its requirements, the next steps were to determine and specify what we needed to do, and to do it. These are discussed in sections 4, What we needed to do (pg.6) and 5, What we did (pg.6). The detailed records of the steps performed and the information archived appear in the appendices of the commercial-in-confidence report. The appendices of this report contain the details of the process, supporting reference material and illustrations of the type of information archived:

Appendix A: Registry files (pg.11)
Appendix B: Summary of information archived Pg 13
Appendix C: Interaction with DSTO-E Registry (pg.13)
Appendix D: Interaction with SCIS (pg.14)
Appendix E: Inside DSTO IPA Branch (pg.18)
Appendix F: Other DSTO (pg.19)
Appendix G: Outside DSTO (pg.20)

1.4 Acknowledgements

Huge thanks to Brian Holland from Defence Support for educating me about records and archives, to Sharolyn Roach for helping with the detail, and to Robert Burgemeister and Martin Foreman of SCIS. Thanks also to Derek Weber for helping find "stuff" and explaining what he'd found, Matt Philips for helping with the analysis, Dale Lambert for interesting, entertaining and insightful discussions and advice, and to Richard Price, Brenton Williams and Dale Lambert for moral and financial support.

2. The Archives Act 1983

The Archives Act 1983 (An Act relating to the preservation and use of archival resources, and for related purposes) addresses the setting up, governance, powers and responsibilities of the National Archives of Australia.

The objects of the Act are:
(a) to provide for a National Archives of Australia, whose functions include:
- (i) identifying the archival resources of the Commonwealth; and
- (ii) preserving and making publicly available the archival resources of the Commonwealth; and
- (iii) overseeing Commonwealth record-keeping, by determining standards and providing advice to Commonwealth institutions; and

(b) to impose record-keeping obligations in respect of Commonwealth records.

The act does NOT define the processes, practices and/or requirements of the Archives themselves, or of the process of archiving information.

Such matters are defined by publications available from the National Archives of Australia website (http://www.naa.gov.au) – refer to Appendix H: National Archives Website (pg21) for more information.

See Appendix L: Archives Act 1983 (pg 40) for more detail regarding the Act.

3. The archive process

3.1 Overview and Issues

I phoned the DSTO-Edinburgh Registry (x97000) and asked "How do I archive something?" After a short discussion, they decided I needed to talk to "the boss".

The Team Leader, Archives & Records phoned me and was *very* helpful. We discussed the matter and the associated implications. He answered my questions, explained the situation and its requirements, and noted that there were a couple of issues he needed to check. He got back to me with the answers later that day, and with a plan of action. He also directed me to the National Archives of Australia website (http://www.naa.gov.au) where I found copies of the various documents, procedures and definitions he referred to in his discussions with me.

The major points of interest were/are:

3.1.1 General information

- The general DSTO-E Registry is in 40Labs.
- There is also a records management and archive facility on site, in 24Labs, which contains 6km of compactus shelf space(!)
- Both are staffed by Defence Support staff – NOT DSTO staff.
- These facilities provide functionalities which are compliant with National Archives of Australia requirements documented in:

  - "Standard for the Physical Storage of Commonwealth Records"
    (refer to Appendix I: (Physical Records) section I.1 page 29)
  - "Digital Recordkeeping: Guidelines"
    (refer to Appendix J: (Digital Records) section J.1 page 33)
- These facilities also comply with DSA standards for storage of classified material.

3.1.2 Records

- The archive process involves archiving "records".
  i.e. That which is to be archived must first become a "record".
- Defence's "records" are recorded in the DRMS – Defence Records Management System – and stored in the appropriate environment that matches the storage and retrieval (and security classification) requirements.
- DSTO staff do not have general access to DRMS; DSTO's records and archives are managed by Defence Support staff (who DO have access to DRMS)
- Once the "record" is recorded in DRMS, and is no longer required locally, it can then be "archived".

3.1.3 DRMS – Defence Records Management System

- Digital records, and information about physical records, are stored as corporate files in DRMS.
- DRMS is implemented as a distributed database, with the DRMS server replicating new and updated information across all nodes in the network with a lag of about 2 hours. If you want access to non-local information more quickly than that, you can remote-login to the non-local machine.
- DRMS is generally available via the DRN.
- A new version of DRMS was installed in early October 2010.
- There is an intention / desire / edict or similar that once this version and its associated processes are bedded in, DRMS will become available to, and will be required to be used by, all of Defence.
- MS Sharepoint use for records management will be replaced by DRMS, not only because DRMS provides more functionality, but also because Sharepoint is NOT an approved / authorised / compliant or similar records management system.

3.1.4 Disposal Authority

- A "Disposal Authority" is a document describing the conditions under which the information defined within the authority must be kept and/or disposed.
  (See Appendix K: "GDA25 – General Disposal Authority", pg 37, for an example.)
- One of the fundamental meta-data attributes of a record is its disposal date.
- The Standard for the Physical Storage of Commonwealth Records (Sect I.1, pg 29) contains more information. For example:
  - Section 1.3 pg 5
    - *Administrative Functions Disposal Authority* (March 2000)
    - agency-specific Records Disposal Authority
  - Section 1.5 pg 6
    - Agencies are strongly encouraged to determine the disposal status of their records at or before creation through the development of functions-based

records disposal authorities. This approach will enable the most appropriate and efficient management strategy to be adopted from the earliest possible point in the record-keeping process. This can include, for example, choosing archival quality paper products to create any paper records that require long-term retention.

3.1.5 Archiving paper records

- Once the "record" is recorded in DRMS, and is no longer required locally, it can then be "archived".
- A record which is to be archived is examined by an archival specialist/expert and assessed against the relevant disposal authority (document). i.e. the process is:
  - Examine the record
  - Determine its value wrt the relevant disposal authority (document)
  - Dispose of it or keep it, and specify the conditions
- The physical aspects of records which are archived are physically transferred to a National Archives of Australia facility.

3.1.6 Archiving non-paper records

- The process for archiving physical "things" is so complex that almost nobody archives them. For example: The DSTO Wind Tunnel people felt that their test models should become part of the National Archives. However, when they looked into the process, they quickly decided that the amount of time, effort and energy required to achieve this was excessive. Instead, they donated the models to the DSTO Museum.
- An exception is magnetic tapes and discs and optical discs. The actual media are treated like they were "just another piece of paper", but as the archive community neither trust the longevity of the media, nor the ability of future-technology to read past-technology media, they also copy the contents of the media into DRMS – as an attachment to the corporate file.

3.2 Summary of the relevant defining documents

- Relevant National Archives of Australia documents include:
  - "Standard for the Physical Storage of Commonwealth Records" (refer to Appendix I: (Physical Records) section I.1 page 29)
  - "Digital Recordkeeping: Guidelines" (refer to Appendix J: (Digital Records) section J.1 page 33)
  - National Archives of Australia, *Why Records Are Kept: Directions In Appraisal*, Canberra, 2000, (http://www.naa.gov.au/records-management/keep-destroy-transfer/why-records-are-kept/index.aspx)
  - National Archives of Australia, "GDA25 – General Disposal Authority" (refer to Appendix K: pg 37, and http://www.naa.gov.au/records-management/IM-framework/outsourcing/GDA25.aspx)
  - National Archives of Australia, *Archives Advice – Preservation* series (www.naa.gov.au/recordkeeping/preservation/advices/preservation.html)
- DSA standards for storage of classified material.
- Attorney-General's Department, *Commonwealth Protective Security Manual*, Canberra, 2000, especially

  - Part C (Information Security),
  - Part D (Personnel Security) and
  - Part E (Physical Security).
- Relevant Acts of Parliament include:
  - The Archives Act 1983 – as revised – see Appendix L: (pg 40)
  - The Crimes Act 1914
  - The Evidence Act 1995
    See H.5 Records in Evidence: The Impact of the Evidence Act (pg 26)
  - The Freedom of Information Act 1982
  - The Privacy Act 1988
- The relevant Standards include:
  - AS 4390 The Australian standard for records management
  - AS 5090 Work Process Analysis for Recordkeeping
  - AS 5044 AGLS (Aus Govt Locator Service) metadata standard
  - AS ISO 15489 Aus and international standard for records management
  - See H.3.1 National and international standards (pg 23)
- Other
  - *Administrative Functions Disposal Authority* (March 2000).
  - Ling, Ted, *Solid, Safe, Secure: Building Archives Repositories in Australia,* National Archives of Australia, Canberra, 1998, Chapters 3 and 6.
  - *General Disposal Authority No. 22 for Records of Short-term Value that have been Copied*, National Archives of Australia, Canberra, 1995.
  - *Privacy Act 1988* and *Crimes Act 1914,* available on the SCALEplus website (scaleplus.law.gov.au/).

4. What we needed to do

Given the complexity and subtleties of the requirements, the Team Leader, Archives & Records offered that Defence Support would do the recording and archiving for us. He suggested that we write our digital "stuff" onto CD and/or DVD, bundle it up with our paper "stuff", and send it all over to Registry staff in 40Labs.

5. What we did

The work involved several threads, each involving a number of steps and interdependencies.

5.1.1 Thread 1: Determine the archiving requirements and process

(no dependencies)

- 1a) Commence determination
- 1b) Complete determination
- 1c) Document findings

Refer to:

  - Section 2 The Archives Act 1983 (pg 3)
  - Section 3 The archive process (pg 3)

5.1.2 Thread 2: Locate all copies of all versions of the software

(no dependencies)

- 2a) Commence determination
- 2b) Complete determination
- 2c) Document findings

Refer to:

- E.1 Locate all copies of all versions (pg 18)
- F.1 Locate copies (pg 19)
- G.1 Identify organisations likely to have a copy (pg 20)

5.1.3 Thread 3: Determine the task requirements and process

Dependent on 1a)

- 3a) Commence determination

Dependent on 1b & 2b

- 3b) Complete determination
- 3c) Document findings

Refer to:

- Section 4 What we needed to do (pg 6)
- Section 5 What we did (pg 6)

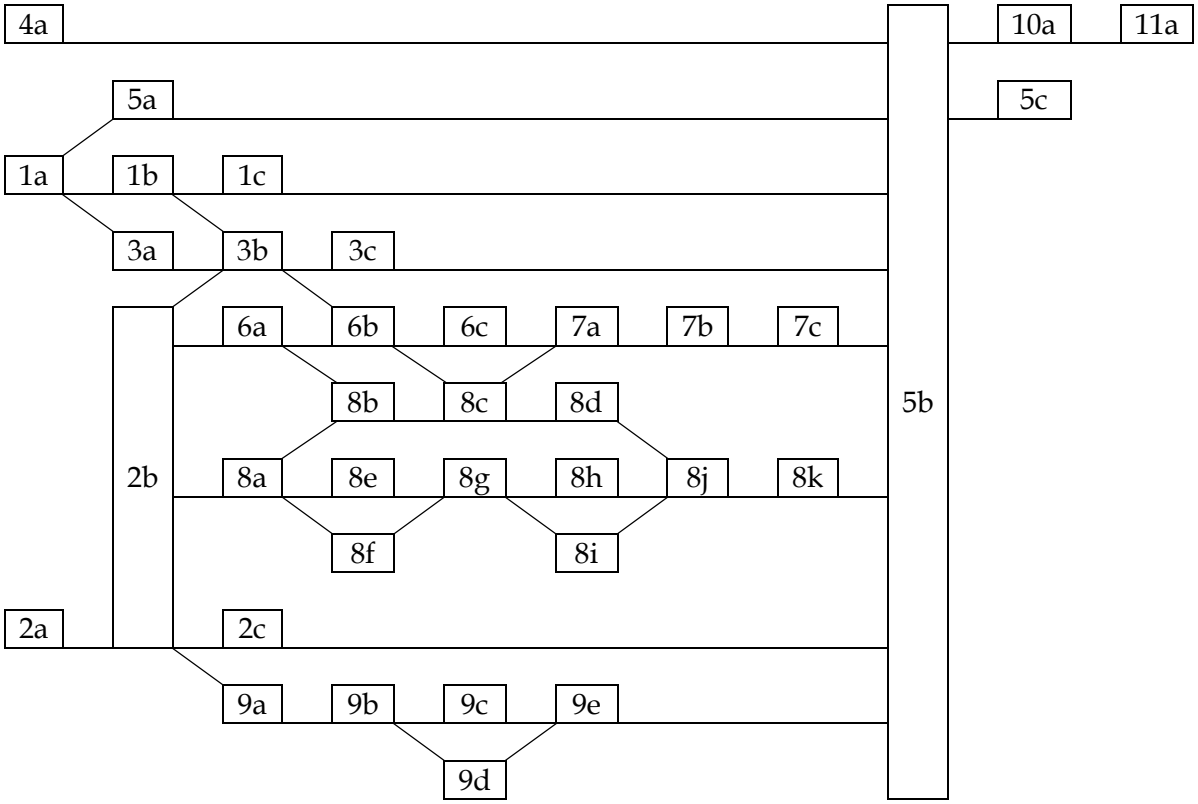

Figure 1 Project task plan showing task dependencies

5.1.4 Thread 4: Open some Registry files

(no dependencies)

- 4a) Open files

Refer to: Appendix A: Registry files (pg 11)

5.1.5 Thread 5: Document the process

Initially dependent on 1a)

- 5a) Commence documenting

Subsequently dependent on ALL other steps except 10a, 11a & 5c

- 5b) Completion of documentation
- 5c) Publication of documentation

5.1.6 Thread 6: Make copies

Dependent on 2b

- 6a) Create copies of information to be archived

Subsequently dependent on 3b

- 6b) Review that copies have been made of all information to be archived
- 6c) Document the information copied

Refer to:

- Appendix B: Summary of information archived (pg 12)
- E.2 Make copies of information to be archived (pg 18)

5.1.7 Thread 7: Archive the information

Dependent on 6c and 8c

- 7a) Package up the information to be archived
- 7b) Send the information to the registry
- 7c) Await feedback from the registry

Refer to:

- Appendix C: Interaction with DSTO-E Registry (pg 13)

5.1.8 Thread 8: Destroy all copies of all versions of the software

Dependent on 2b

- 8a) Approach all points of contact of organisations with copies of the software
- If internal,

  Dependent on 6a
  - 8b) Retrieve any media, ensure a copy has been made, (if necessary, make copies), delete or witness deletion of the software

  Subsequently dependent on 6b
  - 8c) Review that copies exist of all files to be archived.
  - 8d) Review that all software has been deleted.
- If external,
  - 8e) retrieve any media or ask them to certify they have destroyed the media
  - 8f) ask them to certify that they have deleted all copies the software
  - 8g) await receipt of certification(s) and media
  - 8h) place certificates on file
  - 8i) destroy media, if any
- 8j) Review 3b – If necessary, revisit earlier steps
- 8k) Document the events

Refer to:

- E.3 Delete copies from shared resources (pg 18)

- E.4 Delete copies from individual machines (pg 18)
- E.5 Delete individual copies from shared resources (pg 18)
- F.2 Delete them (pg 19)
- G.2 Ask them to delete copies and provide us with a confirming letter (pg 20)

5.1.9 Thread 9: Implement "recovery monitoring" systems

Dependent on 2b

- 9a) Determine relevant backup policies
- 9b) Determine and agree "recovery monitoring" systems
- 9c) Document agreements
- 9d) Verify implementation of the "recovery monitoring" systems
- 9e) Document the events

Refer to:

- Appendix C: Interaction with DSTO-E Registry (pg 13)
- Appendix D: Interaction with SCIS (pg 14)

5.1.10 Thread 10: Completion of task

Dependent on completion of 5b (i.e. dependent on all other steps except 5c and 11a)

- 10a) Task completed. (The task was completed in January 2011)

5.1.11 Thread 11: Ongoing

Dependent on 10a

- 11a) Periodic verification of the implementation of the "recovery monitoring" systems

Refer to:

- Appendix C: Interaction with DSTO-E Registry (pg 13)
  - C.2 Summary of interaction (pg 13)
- Appendix D: Interaction with SCIS (pg 14)
  - D.5 Summary of plan agreed with SCIS (pg 16)

6. Summary and conclusions

Given the knowledge and helpfulness of the Records staff, the actual task of archiving was not particularly arduous. The hard parts of the job were working out what all of the other requirements were, (and there were surprisingly many), and of identifying and gathering all of the information prior to archiving it. As with many such tasks, "the devil is in the detail". It is hoped that this report will reduce the burden for others performing such a job.

7. References

- Section 3.2, Summary of the relevant defining documents (pg.5) contains the details of 22 documents which address:
  - Relevant National Archives of Australia documents.
  - DSA standards for storage of classified material.
  - Attorney-General's Department, *Commonwealth Protective Security Manual*
  - Relevant Acts of Parliament
  - Relevant Standards
- Appendix A: (pg.11) lists the Registry files relevant to this report.

- Section D.5 (pg.16) contains a Summary of plan agreed with SCIS
- Section E.2 (pg.18) summarises all of the information that was found and archived
- Appendix H: (pg.21) summarises the information on the National Archives Website

Appendix A: Registry files

This appendix is used to record the list of relevant Registry files.

The layout of this document is intended as a template that can be used to facilitate achievement of providing a record, (and hence evidence), of the work done – in order to demonstrate that the tasks were performed, and that they were performed with due diligence. Accordingly, details and specifics have been removed.

A.1. Commercial-in-Confidence Registry files

A.1.1 The archiving of the Xxxx software and associated data

This file contains the documentation and correspondence regarding the archive process.
Security Classification: Unclassified - Caveat: Commercial-in-Confidence
File Number: 2010/nnnnnnn/1

A.1.2 Archive of the Xxxx software and associated data

This is the "thing" that was entered into DRMS and archived. It is an A4 ring binder containing the collection of CDs and DVDs which contain the various files described in Appendix B: Summary of information archived of this report.
Security Classification: Unclassified - Caveat: Commercial-in-Confidence
File Number: 2010/nnnnnnn/2

A.1.3 Report of the archiving of the Xxxx software and associated data

The registry file for the report DSTO-GD-xxxx. The report records the details of what was done, and what was archived.
Security Classification: Unclassified - Caveat: Commercial-in-Confidence
File Number: 2010/nnnnnnn/3

A.2. Unclassified Registry Files

A.2.1 Archiving a Software Development Project

The registry file for this report. (DSTO-GD-zzzz) This report records the procedures and processes required for the archiving of a DSTO Task involving software development.
Security Classification: Unclassified – no caveats / general release
File Number: 2010/1141598/1

Appendix B: Summary of information archived

This appendix is used to record the list of data archived, the types of media used for the archiving, and the contents of each of the items used.

The layout of this document is intended as a template that can be used to facilitate achievement of providing a record, (and hence evidence), of the work done – in order to demonstrate that the tasks were performed, and that they were performed with due diligence. Accordingly, details and specifics have been removed.

The following is a list of the CDs, their top level directories, and a summary of their contents.

<Detail removed>

Appendix C: Interaction with DSTO-E Registry

C.1. DSTO-E Records Management Personnel

The first point of contact is either with Registry staff (x97000), or with

- Team Leader, Archives & Records,
  Defence Support - Central and West,
  Bldg 24L, DSTO-E,
  Phone: (08) 7389 6493
  Mobile: 0418 347 747
  Fax: (08) 7389 7967

C.2. Summary of interaction

Initial contact with the Team Leader, Archives & Records is summarised above. (Section 3.1, pg 3)

Registry files created are summarised above. (Appendix A: Registry files, pg 11)

The details of the requirements, and of the steps in the process, were discussed and arranged with Registry staff located in Bldg 40L, DSTO-E. (x97000)

As a result of these discussions, an A4 ring binder [containing the collection of CDs and DVDs which contain the various files described in **Error! Reference source not found.**of this report] was handed to Registry staff who entered it into DRMS and archived it. In the DRMS, it is treated as a DSTO registry file,

Security Classification: Unclassified - Caveat: Commercial-in-Confidence
File Number: **2010/nnnnnnn/2**

but with some "special handling" requirements, in particular: Any requests to access the file generate an "alert" to registry staff, and a semi-automatic email to me. A copy of an example of an alert email has been placed on file 2010/nnnnnnn/1.

Appendix D: Interaction with SCIS

D.1. Determine backup policies and practices

Task: *For each system and/or group of files:*

- *Identify the people responsible for backup policy and for the performance of backups*
- *From them, determine the backup policies and practices*
- *With them, develop a plan for implementing the removal of Xxxx related files from the backups, and for implementing "recovery monitoring".*

D.1.1 Locally managed servers

`<Detail removed>`

D.1.2 Everything else

"Everything else" of interest to us is:

- I & H drives
- gForge

These are all managed by SCIS. After discussions with SCIS, I discovered the information summarised in this appendix, and SCIS officers and I agreed on the plan described in section D.5 below.

D.1.3 Summary of SCIS backup regime

SCIS do a full backup every week and an incremental backup nightly. Their tape library provides a twelve week cycle – in week 13 they reuse the tapes from week 1. Hence, SCIS can only restore data that has been in existence some time in the last 12 weeks. SCIS do *not* provide an archiving service – archiving is the responsibility of the data owner. All of the data mentioned (in section D.1.2 above) is under this regime.

The backup system is managed by software. Thus, although retrieval is limited to 12 weeks, because of the backup software systems design, it is possible that some fragments of data may be in the backup system for up to 23 weeks.

D.2. Discuss "recovery monitoring" with SCIS

Topics:

- **Specification / definition of "recovery monitoring"**

Task: *This involves the automatic generation of an "alarm" should anyone not authorised by CC3ID (or his delegate) attempt to:*

- *Retrieve a backup of Xxxx related files*
- *Retrieve deleted Xxxx related files from a disk*

- **Implementation of "recovery monitoring"**

Task: *The task is to monitor the implementation of "recovery monitoring" of Xxxx related files.*

- **Review of "recovery monitoring"**

Task: *The task is to set up a process which periodically reviews the "recovery monitoring" system.*

Refer to the other sections of this appendix for the outcomes of these discussions.

D.3. Summary of "recovery monitoring" issues

D.3.1 Recovery of files from backup

The 12 week backup cycle, and the lack of archives makes the addressing of this issue quite simple. Refer to section D.5 below for the method chosen.

D.3.2 Recovery of deleted files from disk

A person wishing to recover a deleted file from disk requires all of:

- **Knowledge**: Knowledge that the file once existed, and of where it was.
- **Skill**: The skills to find all of the bits that made up the file, to retrieve them, and to put the segments back together in the right order.
- **Access**: Both physical and logical access to the resources involved.
- **Motivation**: The person involved must want to do it, be prepared to expend the effort required to do it, and be prepared to manage and accept the risks (& consequences) of getting caught. The combination of the perceived benefits and chance of success needs to exceed the combination of the perceived costs and risks.
- **Luck**: All of the disk segments that were used by the deleted file must not yet have been overwritten by new files. (In certain circumstances, partial recovery of a file may be acceptable, but for software, complete recovery is necessary.)
- **Opportunity**: The person involved must be able to place themselves in the right place and the right time, for long enough to be able to successfully complete the task.

I can not think of anyone who would have the motivation to want to retrieve what is now an old version of the software, even if doing so was a simple task. However, assuming that there is such a person, and also assuming that all of the necessary disk segments were still intact (which, by the way, is most unlikely), the likelihood that this person has all four of the knowledge, the skill, the access and the opportunity to resurrect a set of files deleted from the DSTO Restricted Network some time ago is microscopic.

Hence, SCIS advise me that the risk of successful undetected recovery of a deleted file from a disk associated with the DSTO Restricted Network is indistinguishable from zero.

D.4. Other issues

However, SCIS informed me of other avenues possibly available to the motivated, the most obvious being: having data stored on a computer's local disk.

There are two methods available to address this: software monitoring and disk scanning.

D.4.1 Software monitoring

Each time a machine connected to the DSTO Restricted Network logs on and runs the login script, the script examines the list of installed software. For each entry in the list, the script records the software identifier, the machine name, the user name, the date & time of login, the date & time the software was installed, the software version number, and other information. These are written into an SQL database.

A SCIS officer searched the database for "Xxxx" and "Xxxx" and found 12 machines – 6 with Xxxx, and 6 with Xxxx.

<Further Detail removed>

D.4.2 Disk scanning

On each machine that I have identified as potentially having had Xxxx or Xxxx installed, I have found someone with administrator rights to the machine's local disk, and got them to run, from the root directory, the script:

dir /s /a *Xxxx* *Xxxx* *Xxxx* > dirsa_Xxxx.txt

(This does a search of the whole disk, and lists all filenames and directory names that include the strings "Xxxx" "Xxxx" "Xxxx".)

The advantage of running this script is that it lists *all* relevant files, whereas a "windows search" will not list some hidden and systems files, even when you have told it to. The script also writes a copy of the output to a file.

If this search has identified anything relevant, I have uninstalled the software, deleted the relevant directories, and then run the script again. I have kept copies of all before and after scans, and these have been written to CD. *<Further Detail removed>*

Additionally, I arranged with C3ID Executive Officer staff for them to run the scan on the entire "I:" drive. (The C3ID file server.) This scan identified that the only files left on the fileserver are *<Detail removed>* – there is no indication of any software remaining on the I: drive.

Scanning the IA Discipline fileserver "lime" verified that the software had been removed from the expected areas, but identified an archive tucked away in an obscure place. These "extras" have been placed on CD and have been removed from "lime".

SCIS advised that they could run the scan over all "H:" drives.

An additional approach would be to have the disk scan script run as part of the SCIS login script. However, as the elapsed time required to scan a whole disk is notable (e.g. ~10 minutes for a 100GB disk), this is not a practical option.

Note that this scan is in no way a foolproof method of finding all copies of the software – if a relevant file does not have "Xxxx" etc. in its name, or is not in a directory with "Xxxx" etc. in its name, then the scan will not identify it. Similarly, if the file is packed up, compressed, and/or encrypted into a file with a non-"Xxxx" name in a non-"Xxxx"-named directory, the scan will not identify that, either. Conversely, the Software Monitoring (section D.4.1) identifies all installed versions of the software.

D.5. Summary of plan agreed with SCIS

The following plan was developed with and agreed by SCIS, and has been implemented by SCIS:

D.5.1 "Recovery" monitoring

As it takes 23 weeks for all signs of all backed-up files to disappear from the backup system, SCIS have implemented a system of monitoring all requests for file restoration from backup in the period 1 January 2011 to 30 June 2011. Any requests to restore files relevant to Xxxx will be refused, and I will be informed. I will bring these requests to the attention of CC3ID and/or his delegate.

D.5.2 Software monitoring

As described in section D.4.1, all installed software is recorded on login to the DSTO Restricted Network. SCIS have implemented a system of monitoring their database to highlight occurrences of the installation "Xxxx" and/or "Xxxx", and advise me if any such installations occur.

D.5.3 Disk scanning

SCIS have arranged to scan all H: drives for files and directories containing the strings "Xxxx", "Xxxx" and "Xxxx" in their names.

Appendix E: Inside DSTO IPA Branch

E.1. Locate all copies of all versions

Various copies of various aspects of various forms of the Xxxx Software Development Project were distributed over a number of locations and computers within the DSTO-E site.

E.1.1 DSTO IPA People involved

<Detail removed>

E.1.2 Etc.

<Detail removed>

E.2. Make copies of information to be archived

All versions of everything found have been copied to CD (rather than DVD) on the anecdotal basis that CDs are more "robust" than DVDs and have a longer life. Given that there is evidence that both CDs and DVDs physically deteriorate with age, and hence neither is particularly suitable for long term archive use, this would indicate a problem. However, as previously mentioned (section 3.1.6 Archiving non-paper records pg 5, 4th bullet), this problem is addressed by copying the contents of the media to DRMS.

E.2.1 Versions of Xxxx located and archived

<Detail removed>

E.2.2 List of CDs burnt and CDs located

Copies of full directory listings of all CDs are stored on CD, *<Detail removed>*

The following is a list of the CDs, and a summary of their contents. A copy of their top level directories can be found in Appendix B: Summary of information archived (pg 12)

<Detail removed>

E.3. Delete copies from shared resources

<Detail removed>

E.4. Delete copies from individual machines

<Detail removed>

E.5. Delete individual copies from shared resources

<Detail removed>

Appendix F: Other DSTO

F.1. Locate copies

Known to have copies:

<Detail removed>

Unlikely to have copies

<Detail removed>

F.2. Delete them

<Detail removed>

Appendix G: Outside DSTO

G.1. Identify organisations likely to have a copy

Known to have copies:
<Detail removed>

May have copies:
<Detail removed>

Unlikely to have copies
<Detail removed>

Known to NOT have copies
<Detail removed>

G.2. Ask them to delete copies and provide us with a confirming letter

<Detail removed>

Appendix H: National Archives Website

http://www.naa.gov.au

The website of the National Archives of Australia is presented in a number of sections. The ones of interest to us are:

- The Collection – tells about the content, nature and scope of the Archives collection
- Records Management – contains information on the general topic, and specific information, (usually in the form of publications) which define the NAA's requirements, processes, practices and procedures.
- Assorted FAQs, in a number of places
- Publications

I have also included the headers of, and pointers to, a number of other subsections of possible interest.

H.1. The Collection

H.1.1 FAQs

http://www.naa.gov.au/collection/faqs/index.aspx

H.1.2 What sorts of records does the National Archives hold?

http://www.naa.gov.au/collection/faqs/index.aspx#sectiontcm:2-5127

For an overview of the types of records we hold you might like to:

- examine the scope of our collection (http://www.naa.gov.au/collection/scope/index.aspx)
- explore the contents of our collection http://www.naa.gov.au/collection/explore/index.aspx
  - Records of defence administration, the forces, service personnel and more http://www.naa.gov.au/collection/explore/defence/index.aspx
  - How the Commonwealth has managed the defence of Australia http://www.naa.gov.au/collection/explore/defence/administration.aspx
  - Other defence administration records http://www.naa.gov.au/collection/explore/defence/administration.aspx#section9
    - Over 500 collections are held dealing with aspects of defence policy and administration. Major Department of Defence collections include those covering the years 1935–58 and 1957–74. Other collections can be identified through searches in RecordSearch.
- browse our fact sheets and other online publications
  - http://www.naa.gov.au/about-us/publications/fact-sheets/index.aspx
  - http://www.naa.gov.au/about-us/publications/fact-sheets/on-defence/index.aspx
  - http://www.naa.gov.au/about-us/publications/fact-sheets/by-number/index.aspx

You can also find out what's not in our collection
http://www.naa.gov.au/collection/scope/not/index.aspx

Commonwealth records are any records that an Australian Government department or agency has created or kept in the course of carrying out its business, including official files or correspondence, registers, manuals, maps, plans, photographs, and electronic records.

H.1.3 Scope

http://www.naa.gov.au/collection/scope/index.aspx

Records in the National Archives come in a range of formats:

- paper files – the bulk of our collection
- photographs – a few hundred thousand
- audiovisual – around half a million film, video and sound recordings
- large-format – maps and plans
- objects – including treasures such as the cigarette case Ataturk gave Prime Minister Stanley Melbourne Bruce
- digital – some agencies have already transferred digital records to the Archives

H.2. Records management

http://www.naa.gov.au/records-management/index.aspx

Records are an essential tool of good business and for efficient administration. They provide:

- information for planning and decision-making
- evidence of government accountability

and are often subject to specific legal requirements.

For government agencies, records document what is done and why. They provide evidence of communications, decisions and actions.

In the long term, some of the records your agency makes will be retained as national archives and so become part of Australia's documentary heritage.

H.2.1 New to Records Management?

http://www.naa.gov.au/records-management/new-to-rm.aspx

If you are a public servant new to working in information and records management and helping other agency staff with these matters, the amount you need to know can seem overwhelming.

The National Archives is here to help you. We have a range of training courses and publications that cover both general and specific topics. There is information on our website and we have an Agency Service Centre to help Australian Government agencies with their records management queries.

H.2.2 Explore the Archives website

Our website is a great place to get an overview of what records management is all about and what your agency needs to have in place. It is organised into broad tasks related to records management that should link you directly with the information you are looking for:

- Information management framework – **Find out what a record is**, why you need to manage records, and what policies and procedures your agency needs to ensure it meets its obligations in relation to government records management.

- IT systems – what you need to know about computer systems that can make and keep records and managing records in existing systems.

- Create, capture and describe – when staff in your agency **need to make a record, where to put it and how it should be described** (including metadata standards such as AGLS, the Australian Government Recordkeeping Metadata Standard, and the Email Metadata Standard).

- Keep, destroy or transfer – **how long to keep records**, and how to destroy or transfer them. This section includes information about accountable destruction of records, how to get a records authority, how to sentence a record using an authority, how to transfer records between agencies or, if the government is privatising aspects of your core business, how to transfer relevant records.

- Secure, store and preserve – **how to secure, store and preserve your records, both physical and electronic.**

- Access – how to make sure your records are findable and readable for as long as they are required. This section contains information on different ways to access records held by the National Archives as well as advice on how to track records within your agency.

There are also useful sections on training and a listing of all of our publications.

The most detailed information is generally found in publications linked from the top-level pages or from the publications page. As you become more experienced you may choose to go directly to the publications page rather than through the main site. Using our search facility in the top right corner of any page or the site map – in the footer – can help you find the information you need.

H.2.3 Take a look at the standard and other publications

For an overview of best practice records management you should familiarise yourself with the Australian Standard for Records Management – AS ISO 15489. Other standards, manuals and guidelines are available under the publications area of our website.

H.3. Guidelines to help you understand recordkeeping requirements

http://www.naa.gov.au/records-management/im-framework/requirements/standards/index.aspx

H.3.1 National and international standards

- **AS 4390 and AS ISO 15489**

The Australian and international standard for records management, AS ISO 15489, provides guidance on creating records policies, procedures, systems and processes to support the management of records in all formats. It is widely used in Australia and internationally in both private and public organisations.

The National Archives of Australia endorses *AS ISO 15489* for use in the Australian Government. This standard provides the basis for all the Archives' records management standards, policies and guidelines.

- **AS 5090**

AS 5090: Work Process Analysis for Recordkeeping is a complimentary standard to *AS ISO 15489: Records Management*. It assists organisations in understanding their work processes so that they can identify their recordkeeping requirements.

- **AS 5044**

The AGLS metadata standard, *AS 5044,* is the national standard for online resource discovery, mandated for use on all Australian Government websites. There is an Australian Government Implementation Manual available for this standard.

H.3.2 National Archives standards

- **Standard for the physical storage of Commonwealth records**

The storage standard is a comprehensive guide to the storage of all Australian Government records, whether held in agency-owned or leased facilities, or with alternative storage providers. The standard covers all types of storage and represents a code of best practice for the storage of government records. The standard is supported by implementation guidelines.

- **Australian Government recordkeeping metadata standard**

The Australian Government recordkeeping metadata standard describes the information Australian Government agencies should incorporate to establish physical and intellectual control over their records.

Compliance with the standard will help agencies meet business, accountability and archival requirements in a systematic and consistent way by maintaining reliable, meaningful and accessible records over time.

- **Guidelines for mobile shelving**

The *Guidelines for mobile shelving* provide information about the practical installation of mobile shelving in archives, libraries and museums.

The National Archives produced these guidelines in association with Standards Australia and Standards New Zealand.

- **Paper testing using Australian and international standards**

Australian Government agencies wishing to print or create paper records that need to be kept for a long time should use archival quality paper.

The National Archives provides a program to analyse paper for its archival quality. Paper endorsed by the Archives as being of archival quality can use the Archival Quality trademark.

- **Other National Archives policies and guidelines**

A full list of the National Archives' policies and guidelines are available through the publications pages of this website.

H.4. Got a specific question or need more help?

If you work for an Australian Government agency and you have any questions about records management matters you can contact the Archives Agency Service Centre. http://www.naa.gov.au/records-management/help/index.aspx

H.4.1 Common queries from Aus Govt agency staff

- What is a record?
- How do I get a copy of a disposal authority?
- Can I have more information on the National Archives digital preservation software?
- Can I use the training package and cartoons from Keep the Knowledge?
- How long do I have to keep back-up tapes?
- What advice do you have about digitising hard-copy records?
- Where can I get information on archiving websites?
- How often should I take a 'snapshot' of my website?
- How do I folio a record?

H.4.2 What is a record?

First answer:
http://www.naa.gov.au/records-management/help/FAQs.aspx#section1#section1

In the Australian Government context, a record is created when people document their work. A record is evidence of a business transaction or decision.

The key distinction between records and other types of business information is that records provide evidence of business activities. Records can be created in all formats. They can be paper or electronic and include reports, minutes, email and spreadsheets. A record does not have to be finalised. Drafts and working papers are records too. Records may relate to critical agency business or they may document routine administrative matters. Information received from other organisations may be evidence of their business activities, but doesn't need to be managed as a record by your agency. If in doubt, treat information as a record and manage it according to your agency's business needs.

When does it become a record?

A record is evidence of a business activity from the time it is first created. If it documents your agency's work it is a record regardless of its format and where and when it is filed. Records are sometimes kept in email folders, shared drives, and on laptop computers or in systems with records management functionality.

Is it a record while it is still being developed?

Although records that are being developed are subject to comment and change, they are still records of the process up to that stage. It's important to know the status of a record – is it the final version, has it been approved yet, or is this an earlier version with the final stored elsewhere? Some agencies develop records in electronic systems such as shared drives, content management systems, or electronic document management systems. In some cases documents are developed in systems that manage versions, in other cases the agency requires only the final version to be stored in a system with records management functionality.

Second answer:
http://www.naa.gov.au/records-management/IM-framework/what-is-a-record/index.aspx

A record is ...

all information created, sent and received in the course of carrying out the business of your agency. Records have many formats, including paper and electronic. Records provide proof of what happened, when it happened and who made decisions. Not all records are of equal importance or need to be kept.

What records need to be kept

Records that relate to high-risk areas of your business require most attention as they need to be kept to provide evidence, to support your actions and to ensure accountability. You should keep the records that support your business decisions and you should manage them appropriately. Advice on this website will help you do this.

What records can be destroyed?

Records should be destroyed in an accountable way using either a National Archives approved Records Authority, a General Disposal Authority or under Normal Administrative Practice.

H.4.3 Info on National Archives digital preservation software

Information on National Archives digital preservation software can be found on our website at the following address. *[I think it's an initiative test ...]* As you can see from this website, you are welcome to download the product from www.sourceforge.net.

We are always looking for organisations to partner with us to build a community of users around our digital preservation products. If you are interested in using our software, or would like to discuss your digital preservation needs, please contact the Agency Service Centre and we can organise for one of our experts to talk to you about preservation in your organisation.

H.4.4 How long do I have to keep back-up tapes?

Computer system back-up tapes can be disposed of when they are no longer required under Normal Administrative Practice, NAP. NAP provides for the destruction of records which are either:

- duplicated
- unimportant or
- only of short term facilitative value.

Computer backup tapes fall into the first and third catagories.

If you are planning to destroy computer back-ups under NAP, you need to ensure that you maintain the original record (i.e. you should only destroy redundant copies) and that destruction is undertaken appropriately. The National Archives has released information on destroying digital records in Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records.

H.5. Records in Evidence: The Impact of the Evidence Act

http://www.naa.gov.au/records-management/IM-framework/requirements/law/evidence.aspx
http://www.naa.gov.au/Images/Records%20in%20evidence%20in%20word%20format%20for%20website%5B1%5D_tcm2-7936.pdf

This publication helps Australian Government agencies manage their records in accordance with the *Evidence Act 1995*. The Electronic Transactions Act affirms the legal status of electronic records and formalises the increasing use of electronic communication in business transactions.

Records in Evidence was produced in cooperation with the Attorney-General's Department, the Office of Government Information Technology and the Tasmanian Department of Premier and Cabinet, Information Strategy Unit.

H.6. IT systems that make, keep and manage records

http://www.naa.gov.au/records-management/systems/index.aspx

Frequently asked questions about IT systems

- Is document management the same as electronic records management?
- Can I use shared folders to manage records?
- How do I manage records that are shared by more than one agency or organisation?
- Frequently asked questions about mobile devices
- What happens to the old records when a new IT system is implemented?
- Are email archiving solutions suitable for managing emails as records?
- What is a collaborative workspace?

Products to help you with IT systems

- Australian Government Recordkeeping Metadata Standard
- Australian Government Recordkeeping Metadata Standard Implementation Guidelines: Exposure Draft
- Check-up: A Tool for Assessing Your Agency's Information and Records Management
- Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records
- Digital Recordkeeping Self-Assessment Checklist
- Designing and Implementing Recordkeeping Systems (DIRKS) Manual
- General Disposal Authority for Encrypted Records Created in Online Security Processes
- General Disposal Authority for Source Records that have been Copied, Converted or Migrated
- Guidelines for Implementing the Specifications for Business Information Systems Software
- Guidelines for Implementing the Specifications for Electronic Records Management Systems Software
- Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption
- Specifications for Business Information Systems Software
- Specifications for Electronic Records Management Systems Software

H.7. Create, capture & describe

Preserving evidence of your business activities

When you create a record you are documenting your business. A record can be a range of different things: a map, written report, email, film or sound recording. The format of the record you create doesn't matter. What is important is that evidence of your activities is recorded in a way that supports your agency's business needs. For further details see Creating records.

As well as creating records, it is essential that staff in your agency capture or save them into your agency's records management systems. This action will ensure that records:

- can be proven to be genuine
- are accurate and can be trusted
- are complete and unaltered
- are secure from unauthorised access, alteration and deletion
- can be found when needed
- are related to other relevant records

For further details see Capturing records.

To enable your records and other information sources to be found and managed over time, you need to add descriptive information about their content and context. This descriptive information is called metadata. For further details see Describe records using metadata.

Products to help you with creating, capturing and describing records

- AGLS Metadata Element Set
- Archiving Web Resources: A Policy for Keeping Records of Web-based Activity in the Commonwealth Government
- Archiving Web Resources: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government
- Australian Government Email Metadata Standard
- Australian Government Implementation Manual for AGLS Metadata
- Australian Government Recordkeeping Metadata Standard
- Australian Government Recordkeeping Metadata Standard Implementation Guidelines: Exposure Draft
- Australian Governments' Interactive Functions Thesaurus (AGIFT)
- Check-up: A Tool for Assessing Your Agency's Information and Records Management
- Developing a Functions Thesaurus: Guidelines for Commonwealth Agencies
- Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records
- Digital Recordkeeping Self-Assessment Checklist
- Designing and Implementing Recordkeeping Systems (DIRKS) Manual
- Guidelines for Implementing the Specifications for Business Information Systems Software
- Introduction to Keyword AAA
- It is your business! Records management is good business and your business
- Making, Keeping and Using Digital Records
- Overview of Classification Tools for Records Management
- Specifications for Business Information Systems Software

H.8. Fact sheet 10 – Access to records

http://www.naa.gov.au/about-us/publications/fact-sheets/fs10.aspx

Contents

H.9. Other pages of interest?

H.9.1 Glossary of records management terms

http://www.naa.gov.au/records-management/glossary/index.aspx

H.9.2 Publications

(Products to help you manage your records (!)
http://www.naa.gov.au/records-management/publications/index.aspx

H.9.3 Training

http://www.naa.gov.au/records-management/training/index.aspx

H.9.4 Keep the Knowledge – Make a Record

http://www.naa.gov.au/records-management/training/Keep-the-Knowledge/index.aspx

Keep the Knowledge – Make a Record is a training package developed by the National Archives of Australia to assist all Australian Government employees, contractors and consultants to understand their records management responsibilities.

Keep the Knowledge can be used by agencies to present in-house training to their staff. Presenting *Keep the Knowledge* in your agency will help staff to:

- identify what is a record
- recognise why records matter
- understand their records management responsibilities
- decide when to make or keep a record
- understand where records should be kept in your agency

Appendix I: Physical Records

I.1. Standard for the Physical Storage of Commonwealth Records

http://www.naa.gov.au/records-management/publications/storage-standard.aspx

Downloadable documents

- Storage Standard (pdf, 123kb)
- Storage Standard (rtf, 721kb)
- Appendix 1: Guidelines for Records Storage (pdf, 89kb)
- Appendix 1: Guidelines for Records Storage (rtf, 589kb)

The Storage Standard describes the recommended conditions under which Australian Government records should be stored, whether they are held in agency-owned or leased facilities or with alternative storage providers. The standard covers all types of storage media including paper, audiovisual material, microforms and machine-readable formats. It represents a code of best practice for the storage of government records and provides a tool to support and improve the management of those records. The standard is supported by implementation guidelines, *Storing to the Standard*.

I.1.1 Table of Contents

I.1.2 Further references

- Ling, Ted, *Solid, Safe, Secure: Building Archives Repositories in Australia,* National Archives of Australia, Canberra, 1998, Chapters 3 and 6.
- *General Disposal Authority No. 22 for Records of Short-term Value that have been Copied*, National Archives of Australia, Canberra, 1995.
- National Archives of Australia, *Archives Advice – Preservation* series (www.naa.gov.au/recordkeeping/preservation/advices/preservation.html).
- Attorney-General's Department, *Commonwealth Protective Security Manual*, Canberra, 2000, especially Part C (Information Security), Part D (Personnel Security) and Part E (Physical Security).
- *Privacy Act 1988* and *Crimes Act 1914,* available on the SCALEplus website (scaleplus.law.gov.au/).

I.2. Storing to the Standard:

Storing to the Standard: Guidelines for Implementing the Standard for the Physical Storage of Commonwealth Records
http://www.naa.gov.au/records-management/publications/storing-to-the-standard.aspx

Downloadable documents

- Storing to the Standard (pdf, 183kb)
- Storing to the Standard (rtf, 1053kb)

These guidelines complement the *Standard for the Physical Storage of Commonwealth Records* and are arranged according to the seven principles outlined in the Standard. They can be used as a checklist to assess whether storage facilities and services satisfy the standard. Together the standard and guidelines provide agencies with a voluntary code of best practice for the storage of Commonwealth records.

I.2.1 Table of Contents

Appendix J: Digital Records

J.1. Digital Recordkeeping: Guidelines

http://www.naa.gov.au/records-management/publications/Digital-recordkeeping-guidelines.aspx

http://www.naa.gov.au/Images/Digital-recordkeeping-guidelines_tcm2-920.pdf
May 2004 - 85 pages

These guidelines provide comprehensive help to Australian Government agencies in creating, managing and preserving their digital records. It will assist staff responsible for digital records and information to manage digital records for as long as they are required.

This publication has a companion. The *Digital Recordkeeping Checklist* is a self-assessment tool for Australian Government agencies to evaluate their management of digital records.

Since releasing the *Digital Recordkeeping Guidelines*, the National Archives has developed generic specifications for agencies wishing to purchase or build Electronic Records Management Systems Software or Business Information Systems Software with records management capability.

http://www.naa.gov.au/records-management/publications/ERMS-guidelines.aspx
http://www.naa.gov.au/records-management/publications/BIS-guidelines.aspx

J.1.1 Executive Summary

Australian Government agencies create many records in digital format. Digital records include word-processed documents, emails, databases and images.

Australian Government agencies are responsible for creating, managing and preserving their digital records for as long as they are required. Agencies should develop an integrated and comprehensive framework for digital recordkeeping.

Digital records are created as evidence of business activity and captured into recordkeeping systems along with metadata that describes their content, structure and context.

Digital records must be managed to remain accessible for as long as they are required. They can be accessed through legislation on archives, freedom of information and privacy. Digital records should be stored in accordance with the frequency of the need to refer to them. Because digital records can be easily modified, their security is very important. Agencies should plan for disasters – loss of digital records can be crippling.

Given the rapid obsolescence of digital technology, agencies should plan for the long-term preservation of digital records. Digital records that are to be retained indefinitely by the agency require preservation to ensure their ongoing accessibility.

Digital records of temporary value must be destroyed securely and in such a way that they cannot be reconstructed. Digital records of archival value should be transferred to the National Archives when immediate business needs have ceased.

J.1.2 Table of Contents

J.2. Making, Keeping and Using Digital Records

http://www.naa.gov.au/records-management/publications/making-keeping-using.aspx
http://www.naa.gov.au/Images/Making_Keeping_Using_tcm2-1236.pdf
2004 - 8 pages – landscape – very colourful – VERY high noise-to-signal ratio

Pg 5 - Our e-permanence suite of tools and guidelines provide the framework for developing systems to make and keep good records – including 'born digital' records. The e-permanence suite is based on the concepts and strategies recommended in the Australian Standard for Records Management, AS ISO 15489.

J.2.1 Keeping Digital Records

Pg 6-7:

We have looked at various Australian and international approaches to the issue of long-term preservation of digital records. Our research indicates that the best strategy is to convert them into a standard, stable format.

Our approach to preserving digital records uses standardised eXtensible Markup Language (XML). Records such as emails, spreadsheets, and word-processed documents created in commercial software programs are converted and stored in a stable, long-term XML form. This enables records to be read with computers now and into the distant future regardless of the format in which they were created. Agencies can transfer digital records of archival value to the National Archives once their immediate business need has ended, for conversion and storage in our digital repository.

We are developing software called Xena (XML Electronic Normalising of Archives) to convert digital records to standardised XML. The Xena software is primarily an internal digital preservation tool of the Archives. However, we are continuing Xena's development as an open source project to enable other parties to enhance the software and use it for their own digital preservation purposes.

Appendix K: GDA25 – General Disposal Authority

http://www.naa.gov.au/Images/GDA25_tcm2-1129.pdf -
Records Issues for Outsourcing including General Disposal Authority 25

CONTENTS

pp 29-33
GENERAL DISPOSAL AUTHORITY NO 25

K.1. The Disposal Process

The disposal of Commonwealth records is the process of assessing the value of records for future use, identifying those which have enduring value and how soon the remainder can be destroyed or otherwise disposed of. The process can also involve the transfer of ownership or custody and the alteration of records. Further, it involves authorising the action arising from the assessment and putting the action into effect.
Section 24 of the Archives Act 1983 provides that records are not to be disposed of without the permission of the National Archives of Australia unless the action of disposal is positively required by law, or takes place in accordance with a normal administrative practice of which the Archives does not disapprove. Advice on the provisions of the Archives Act is available from any of National Archives of Australia offices.

K.2. Purpose of this Authority

This General Disposal Authority authorises the transfer of the custody of Commonwealth records to private contractors providing services, either on behalf the Commonwealth or to the Commonwealth. It also authorises the transfer of ownership of copies of certain records to a contractor.
This Authority also endeavours to protect the rights of the Commonwealth and its citizens by requiring that appropriate measures are in place before records are transferred out of Commonwealth custody.
Only those records which are reasonably required by the contractor to fulfil their obligations should be transferred. All other records should be retained by the agency. The remaining records should be sentenced in accordance with applicable Records Disposal Authorities,

issued by the Archives, and disposed of accordingly (either by destruction or transfer to appropriate storage facilities).
Other than copies of records, this Authority does not authorise the transfer of ownership of any records. If you feel that it is necessary to transfer the ownership of any other records to the contractor, please contact your local office of the National Archives of Australia to obtain advice and authorisation.

K.3. Conditions attached to Authority

The transfer of custody of the records is only valid if the terms and conditions listed in the authority are met. These terms and conditions are to ensure that the agency's obligations under the Privacy Act 1988, Archives Act 1983, Freedom of Information Act 1982, Crimes Act 1914 and any other legislation are met.
Other terms and conditions may be included in contractual arrangements entered into by the agency if required.
It is the agency's responsibility to ensure that all conditions attached to the transfer are met.

K.4. Authorisation

GENERAL DISPOSAL AUTHORITY 25

K.4.1 Person to whom notice of authorisation is given:

Secretaries of Departments, Heads of Authorities and Commonwealth controlled companies (as listed in attachment A to the memorandum 1998/27 dated 5 March 1998 accompanying this Authority)

K.4.2 Purpose:

Authorises arrangements for the disposal of records in accordance with section 24(2)(b) of the Archives Act 1983

K.4.3 Application:

Transfer of custody or ownership of records to contractors providing services on behalf of or to Government under outsourcing arrangements

This authorisation applies to only the disposal of the records described on the authority in accordance with the disposal action specified on the authority. The authority will apply only if disposal takes place with the consent of the agency that is responsible at the time of disposal for the functions documented in the records concerned.

M Piggott 5 March 1998
Authorising Officer,
Australian Archives

Michael Piggott
Director
Disposal Policy and National Coordination
Government Services

K.5. Classes

GENERAL DISPOSAL AUTHORITY 25

Entry 1

Description of Records

Commonwealth records in existence at contract start date reasonably required by the contractor to perform its contractual obligations.

Disposal Action

Transfer custody of records to contractor for the period of the contract provided that the terms and conditions listed below are met.

Terms and Conditions

The Agency must:

- ensure that the contractor does not destroy or otherwise dispose of records without the express permission of the Agency (in accordance with Records Disposal Authorities issued by the Australian Archives);
- recover all Commonwealth records at the completion or termination of the contract, or at any other reasonable time;
- ensure that the records are appropriately managed and maintained;
- ensure that the security of the records is protected;
- ensure that personal information is protected consistent with the provisions of the *Privacy Act 1988*;
- ensure that unauthorised disclosure of information is prevented, in accordance with the provisions of the *Crimes Act 1914* and any legislation relevant to the Agency;
- the contractor provides reasonable access to the records by the Commonwealth and its authorised agents;
- ensure that the use of the records by the contractor is limited to legitimate purposes under the terms of the outsourcing arrangement.

Entry 2

Description of Records

Copies of: operating manuals, procedures, guidelines, publications, handbooks, etc that are required by the contractor to perform contractual obligations

Disposal Action

Transfer ownership to contractor.

Appendix L: Archives Act 1983

L.1. Title

An Act relating to the preservation and use of archival resources, and for related purposes

L.2. 1 Short title

This Act may be cited as the Archives Act 1983.

L.3. 2A Objects of this Act

The objects of this Act are:
(a) to provide for a National Archives of Australia, whose functions include:
- (i) identifying the archival resources of the Commonwealth; and
- (ii) preserving and making publicly available the archival resources of the Commonwealth; and
- (iii) overseeing Commonwealth record-keeping, by determining standards and providing advice to Commonwealth institutions; and

(b) to impose record-keeping obligations in respect of Commonwealth records.

L.4. Summary

The act addresses the setting up, governance, powers and responsibilities of the National Archives of Australia.

It does NOT define the processes, practices and/or requirements of the Archives themselves, or of the process of archiving information. Such matters are defined by publications available from the National Archives of Australia website (http://www.naa.gov.au) – refer to Appendix H: National Archives Website (pg21) for more information.

L.5. Resources/Sources

- http://en.wikipedia.org/wiki/National_Archives_of_Australia
- http://www.austlii.edu.au/au/legis/cth/consol_act/aa198398/
  - http://www.austlii.edu.au/au/legis/cth/consol_act/aa198398.txt/cgi-bin/download.cgi/download/au/legis/cth/consol_act/aa198398.rtf
- http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/A2D2456639992118CA2570C90011F85E?OpenDocument)

L.6. Table of Contents of the act

L.6.1 PART I--PRELIMINARY

L.6.2 PART II--ESTABLISHMENT, FUNCTIONS AND POWERS OF THE NATIONAL ARCHIVES OF AUSTRALIA

L.6.3 PART III--THE DIRECTOR-GENERAL AND STAFF OF THE ARCHIVES

L.6.4 PART IV--NATIONAL ARCHIVES OF AUSTRALIA ADVISORY COUNCIL

L.6.5 PART V--COMMONWEALTH RECORDS

Division 1--Preliminary

Division 2--Dealings with Commonwealth records

L.6.7 PART VII--CARE OF MATERIAL OF THE ARCHIVES

L.6.8 PART VIII--REGISTERS AND GUIDE RELATING TO ARCHIVES

L.6.9 PART IX--MISCELLANEOUS

L.7. Selected sections of the act

L.7.1 2A Objects of this Act

The objects of this Act are:

(a) to provide for a National Archives of Australia, whose functions include:

(i) identifying the archival resources of the Commonwealth; and

(ii) preserving and making publicly available the archival resources of the Commonwealth; and

(iii) overseeing Commonwealth record-keeping, by determining standards and providing advice to Commonwealth institutions; and

(b) to impose record-keeping obligations in respect of Commonwealth records.

L.7.2 3C Director-General may determine archival resources of the Commonwealth

(1) The Director-General may, in writing, determine that a specified Commonwealth record or other material is part of the archival resources of the Commonwealth.

Note: The Director-General may specify a record by reference to a class of records (see subsection 46(3) of the *Acts Interpretation Act 1901*).

(2) The Director-General must not make a determination under this section unless he or she is satisfied that the specified Commonwealth record or other material is part of the archival resources of the Commonwealth (within the meaning of subsection 3(2)).

(3) A determination under this section may be set out in the same document as a permission or approval given under paragraph 24(2)(b) or a notice of disapproval given under paragraph 24(2)(c).

(4) A determination under this section is not a legislative instrument.

L.7.3 6A Records that are not part of the archival resources of the Commonwealth

(1) Nothing in this Act requires the Archives to accept the care of a Commonwealth record that has not been determined to be part of the archival resources of the Commonwealth under section 3C.

(2) If:

(a) a Commonwealth institution has transferred a Commonwealth record to the care of the Archives; and

(b) the record has not been determined to be part of the archival resources of the Commonwealth under section 3C;

the Archives may:

(c) if another Commonwealth institution has succeeded to the relevant functions of the institution—cause the record to be transferred to the custody of that successor institution, but only in accordance with arrangements agreed to by that successor institution; or

(d) otherwise—cause the record to be transferred to the custody of the institution, but only in accordance with arrangements agreed to by the institution.

L.7.4 21 Archives may be given custody of certain records

(1) Subject to any regulations made in accordance with section 20, a person having the control of the custody of any records referred to in section 18 or subsection 19(1) may enter into arrangements with the Archives with respect to the custody of those records.

(2) Arrangements referred to in subsection (1) relating to the custody of records may provide for the extent (if any) to which the Archives or other persons are to have access to those records.

L.7.5 27 Transfer of certain Commonwealth records to care of Archives

(1) This section applies to a Commonwealth record that:

(a) is in the custody of a Commonwealth institution other than the Archives; and

(b) has been determined to be part of the archival resources of the Commonwealth under section 3C.

Note: In certain circumstances a Commonwealth institution or Minister can exempt a record from this section (see section 29).

(2) The person responsible for the custody of the record must cause the record to be transferred to the care of the Archives in accordance with arrangements approved by the Archives.

(3) The record must be transferred:

(a) if the record ceases to be a current Commonwealth record—as soon as practicable after the record ceases to be a current Commonwealth record; and

(b) in any event—within 25 years of the record coming into existence.

L.7.6 39 Information as to existence of certain documents

(1) Nothing in this Act shall be taken to require the Archives to give information as to the existence or non-existence of a record where information as to the existence or non-existence of that record, if included in a Commonwealth record, would cause that last-mentioned record to be an exempt record by virtue of paragraph 33(1)(a), (b) or (e).

(2) Where an application to the Archives for access to a record relates to a record that is, or if it existed would be, of a kind referred to in subsection (1), the Archives may give notice in writing to the applicant that the Archives neither confirms nor denies the existence, as a Commonwealth record, of such a record but that, assuming the existence of such a record, it would be an exempt record, and, where such a notice is given:

(a) section 40 applies as if the decision to give such a notice were a decision referred to in that section; and

(b) the decision to give the notice shall, for the purposes of Division 4, be deemed to be a decision of the Archives refusing to grant the applicant access to the record on the ground that the record is an exempt record under paragraph 33(1)(a), (b) or (e), as the case may be.

L.7.7 62 Samples of material for Archives

(1) The Minister may, by notice published in the *Gazette*, declare that a specified class of objects, not being objects referred to in subsection (3), (4) or (5), is a class to which subsection (2) applies.

(2) The Archives may require any Commonwealth institution to cause to be transferred to the care of the Archives samples of objects included in a class of objects to which this subsection applies that are the property of the Commonwealth or of the Commonwealth institution.

(3) The Reserve Bank of Australia shall cause to be transferred to the care of the Archives such samples as the Archives requires of notes printed by, or under the authority of, the bank that are legal tender throughout the Commonwealth.

(4) The Controller of the Royal Australian Mint shall cause to be transferred to the care of the Archives such samples as the Archives requires of current coins caused by the Treasurer to be made.

(5) The Australian Postal Corporation shall cause to be transferred to the care of the Archives such samples of current postage stamps issued by the Corporation as the Archives requires.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Archiving a Software Development Project

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Peter Fisher

5. CORPORATE AUTHOR

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-GD-0739	AR-015-589	General Document	April 2013

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2010/1141598/1	NS07/201	Exec Dir CSTSC	52	22

DSTO Publications Repository

http://dspace.dsto.defence.gov.au/dspace/

14. RELEASE AUTHORITY

Chief, Command, Control, Communications and Intelligence Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS http://web-vic.dsto.defence.gov.au/workareas/library/resources/dsto_thesaurus.shtml

Software, Archiving, Intellectual Property rights

19. ABSTRACT

The process of archiving Australian Government Records in the National Archives of Australia is non-trivial. Archiving a Department of Defence Software Development Project has added complexities. This document describes and illustrates the steps involved in the archiving of such a project. It also records the process and the issues to be considered, with the intention that others directed toward such a task will not need to rediscover the process and its requirements.