Australian Government

National Archives of Australia

Records Authority

Department of Defence – Information Security

Job no 2009/00120068

October 2009

CONTENTS

[This page has been left blank intentionally.]

INTRODUCTION

The Department of Defence and the National Archives of Australia have developed this Records Authority to set out the requirements for keeping or destroying records for the core business area of Information Security. It represents a significant commitment on behalf of the Department of Defence to understand, create and manage the records of its activities.

As the National Authority for Information Security, the Defence Signals Directorate (DSD) was the principal Department of Defence area involved in the development of this Records Authority. At the time this Records Authority was issued, two other areas had extensive involvement in Information Security: The Defence Cryptographic Controlling Authority (DCCA) and the Australian Defence Force (ADF) Communications Security (COMSEC) Facilities.

This Authority is based on the identification and analysis of the business of the Department of Defence. It takes into account the agency's legal and organisational records management requirements, and the interests of stakeholders, the agency and the National Archives of Australia.

This Authority gives the Department of Defence permission under the Archives Act 1983, for the destruction, retention or transfer to the National Archives of Australia of the records described. The Authority sets out those records that need to be retained as national archives and the minimum length of time that temporary records need to be kept. Retention periods for these temporary records are based on: an assessment of business needs; broader organisational accountability requirements; and community expectations, and are approved by the National Archives of Australia on the basis of information provided by the agency.

The Department of Defence may use the following tools to dispose of their records:

- This Records Authority covering its agency specific records;

- General disposal authorities, such as the Administrative Functions Disposal Authority (AFDA), covering business processes and records common to Australian Government agencies; and

- Normal administrative practice (NAP) which allows for the destruction of records where the records are duplicated, unimportant or for short-term use only.

As changes in circumstances may affect future records management requirements, the periodic review of this Authority is recommended. All amendments must be approved by the National Archives.

Advice on using this Authority and other records management matters is available from the National Archives' website at www.naa.gov.au or by contacting the Agency Service Centre at recordkeeping@naa.gov.au or (02) 6212 3610.

APPLICATION OF THIS AUTHORITY

1. This Authority replaces Records Disposal Authority (RDA) 853 issued in 1992. The superseded RDA may not be used by the Department of Defence to sentence records after the date of issue of this Authority.

2. This Authority should be used in conjunction with the Administrative Functions Disposal Authority (AFDA) issued by the National Archives to cover administrative records common to Australian Government agencies.

3. This Authority should be used in conjunction with general disposal authorities issued by the National Archives that cover other types of records that may be created by the Department of Defence, such as encrypted records and source records that have been copied.

4. This Authority is to be used to sentence records. Sentencing involves the examination of records in order to identify the individual disposal class to which they belong. This process enables sentencers to determine how long records need to be kept. Advice on sentencing is available from the National Archives.

5. Where the method of recording information changes (for example from a manual system to an electronic system, or when information is migrated from one system to a new system) this Authority can still be used to sentence the records created, providing the records document the same core business. The information must be accessible for the period of time prescribed in this Authority. The Department of Defence will need to ensure that any software, hardware or documentation required to enable continuing access to the information is available for the periods prescribed.

6. In general, retention requirements indicate a minimum period for retention. The Department of Defence may extend minimum retention periods if it considers that there is an administrative need to do so, without further reference to the National Archives. Where the Department of Defence believes that its accountability will be substantially compromised because a retention period or periods are not adequate, it should contact the National Archives for review of the retention period.

7. The Department of Defence may destroy certain records without formal authorisation as a normal administrative practice. This usually occurs where the records are duplicated, facilitative or for short-term use only. NAP does not replace the arrangements agreed to in authorities. Advice and guidance on destroying records as a normal administrative practice is available from the National Archives' website at www.naa.gov.au.

8. From time to time the National Archives will place a freeze on some groups of records to prevent their destruction. Further information about disposal freezes and whether they affect the application of this Authority is available from the National Archives website at www.naa.gov.au.

9. Records in the care of the Department of Defence should be appropriately stored and preserved. The Department of Defence needs to meet this obligation to ensure that the records remain authentic and accessible over time. Under section 31 of the Archives Act 1983, access arrangements are required for records that become available to the public after thirty years.

10. Appropriate arrangements should be made with the National Archives when records are to be transferred into custody. The National Archives accepts for transfer only those records designated as national archives.

11. Advice on how to use this Authority is available from the Department of Defence Intelligence and Security Group. If there are problems with the application of the authority that cannot be resolved, please contact the National Archives.

CONTACT INFORMATION

For assistance with this authority or for advice on other recordkeeping matters, please contact National Archives' Agency Service Centre.

Queen Victoria Terrace
Parkes ACT 2600
PO Box 7425
Canberra Mail Centre ACT 2610

Tel: (02) 6212 3610
Fax: (02) 6212 3989
Email: recordkeeping@naa.gov.au
Website: www.naa.gov.au

AUTHORISATION

RECORDS AUTHORITY

Person to whom notice of authorisation is given:	Dr Ian J Watt Secretary Department of Defence RUSSELL ACT 2600
Purpose:	AUTHORISES ARRANGEMENTS FOR THE DISPOSAL OF RECORDS IN ACCORDANCE WITH SECTION 24(2)(b) OF THE ARCHIVES ACT 1983
Application:	INFORMATION SECURITY

This authorisation gives permission for the destruction, retention or transfer to the National Archives of Australia of the records described. The authorisation will apply only if these actions take place with the consent of the agency responsible for the core business documented in the records.

Authorising Officer

Ross Gibbs.

Ross Gibbs
Director-General
National Archives of Australia

Date of issue:

28 October 2009.

[This page has been left blank intentionally.]

INFORMATION SECURITY

Information Security is the business of administering guidelines and standards for the protection of Australian Government Information Communication Technology (ICT) networks and information systems from unauthorised access and other potential threats. It includes providing material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means. It also includes conducting research into cryptology and monitoring compliance with government security policy and providing advice and assistance to Australian Government and organisations that form part of the National Information Infrastructure (NII).

Tasks that support the business of Information Security include:

- policy, liaison, research, development, industry collaboration, communication security monitoring, testing and reporting;
- provision of guidelines and interpretation supporting government regulations and policies relating to Information Security;
- evaluation of Information Security products in accordance with internationally recognised standards;
- oversight of licensed commercial evaluation services;
- certification, accreditation, reviews and audit of Information Security systems for compliance with Australian Government Information and Communication Technology Security Instructions (also known as ACSI);
- investigations and control of Information Security incidents;
- investigation and control of emissions from information technology networks and equipment;
- threat assessment and vulnerability analysis of information technology networks and equipment;
- advice and assistance to Commonwealth and State authorities concerning cryptography, communications technology and other Information Security products;
- plan, coordinate and approve the production, distribution and management of hard copy and electronic traditional key and modern keying material, and other cryptographic products;
- consulting services to assist planning, implementation and operation of appropriate security policies, solutions and practices;
- registration and endorsement of information communication technology assessors;
- registration (licensing) of information communication technology facilities to perform evaluation services;
- controlled access for agencies to security materials, equipment, information systems;
- Information Security training and awareness services; and
- promotion of and dialogue about Information Security through presentations, committees and other representatives.

For records relating to accreditation, certification and advice for ICT breach investigations, threat assessments, computer network vulnerability of ICT systems classified SECRET and below within Department of Defence, use Defence Security Records Authority (job no 2005/00170070).

For all intelligence activities, use General Disposal Authority (GDA) 21.

INFORMATION SECURITY

Entry	Description of records	Disposal action
20078	Records documenting advice, policy, instructions and other Information Security business provided to Commonwealth, State and Territory government agencies that is principal or critical to high level decisions or is of Government /agency wide significance or that results in major changes. Includes: • whole of Government initiatives such as the electronic security (E-security) national agenda and critical infrastructure protection such as the National Information Infrastructure; • development and establishment of overall policy and procedures underpinning the Information Security business and provision of guidelines and interpretation supporting government regulations and policies relating to Information Security; • coordination and management of Information Security related research programs involving partner agencies and research organisations; • monitoring and testing the security of Australian Government communications and systems, which includes Ministerial authorisations; • strategic policy, advice and reporting on whole of Government initiatives including significant policy derived from certification, accreditation, reviews and audits of information security systems for compliance with Australian Government Information and Communication Technology Security Instructions (ACSI); • investigations and control of Information Security incidents associated with major security breaches. Major breaches include removal of highly classified material or equipment from official custody; loss of information; actual or suspected compromise of information including tampering with security equipment or material; actual or suspected hacking into or tampering of any information system or equipment; continuous minor security incidents where the combination of the incidents warrants an investigation; theft and attempted theft of classified equipment or material. Security incidents/investigations may include: Breach reports; Incident reports; Investigation process; and Investigation findings; • final version or master set of Australian Government Information and Communication Technology Security Instructions (also known as ACSI). Includes final approval and significant updates or amendments such as changes to format and where significant consultation with Government and industry stakeholders is required; • promotion of and dialogue about Information Security through high level presentations, committees and other representations including records of committees or bodies where the National Authority provides the secretariat or provides significant input; and • master copy/final version of major lectures, briefs and presentations delivered by senior executive (SES) staff.	Retain as National Archives

INFORMATION SECURITY

Entry	Description of records	Disposal action
20079	Australian Government Information and Communication Technology Security Instructions (also known as ACSI) *Excludes records identified as Retain as National Archives.* Records documenting the process of developing and promulgating the Australian Government Information and Communication Technology Security Instructions. Includes: • required planning and developed work by sponsoring area; • principles and scoping approval; • draft reproduced by sponsoring area; and • draft authorisation.	Destroy 20 years after action completed
20080	Records documenting technical evaluation, assessment, monitoring reporting, advice and liaison with companies/organisations and other interested parties regarding the selection and use of products providing cryptographic services. *Excludes records identified as Retain as National Archives.* Includes: • evaluation advice including the selection and use of products providing cryptographic services, both commercial and government furnished (high grade) equipment; and • suitability of exporting and use of Australian cryptographic goods to overseas countries, including: ▪ register application; ▪ assess cryptographic products applications; ▪ liaise with companies; and ▪ processing assessment sheet including registration number for product export.	Destroy 15 years after action completed

INFORMATION SECURITY

Entry	Description of records	Disposal action
20113	Administrative and operational records documenting the activities associated with the Information Security business, *Excludes records identified as Retain as National Archives.* Includes: • research and development, joint ventures and collaboration. Includes records documenting arrangements, agreements and memorandum of understandings, negotiations with research institutes and industries about Information Security products. Includes: research requirements; initiating and directing research projects; and provision of reports. • minor security incidents investigations. Includes records documenting investigations into minor breaches, unauthorised access and other occurrences which results in negative consequences for the Commonwealth or events that has actual or potentially adverse effects on an information system or equipment. Includes: ▪ requests; ▪ minor breach report; ▪ investigation process; ▪ investigation findings; ▪ correspondence; and ▪ instructions. • threat and vulnerability assessments. Includes records documenting the threat and vulnerability analysis/assessments of Australian government information systems and networks. Includes: ▪ Assessment and analysis of threats to Australian National Information Infrastructure; ▪ Identifying security deficiencies, and effectiveness of proposed security measures implementation. • training records documenting the activities associated with all aspects of training (external/internal) such as implementing accredited Agency Security Adviser (ASA) and Information Technology Security Adviser (ITSA) training courses. Includes liaison and providing advice and assistance to educational institutions. • provision of services for Australian Government networks, gateways and computer equipment and facilities. Includes records of ▪ endorsement and registration of Assessors under the Registered Assessor Program; ▪ licensing of evaluation facilities; ▪ examination and control of compromising emissions from Information Technology networks, equipment and facilities; and ▪ Tempest testing reports for emanation security.	Destroy 10 years after action completed

INFORMATION SECURITY

Entry	Description of records	Disposal action
20114	Original briefing and debriefing certificates for access to Communication Security (COMSEC) or cryptographic material/equipment.	Destroy 10 years after debriefing
20115	Records documenting lower level forums, committees, bodies, working parties, working groups, task forces, conferences and seminars dealing with the Information Security business where the National Authority or the Defence Cryptographical Controlling Authority does not provide the secretariat, or is not the main representative or does not play a significant role. *Excludes records identified as Retain as National Archives.* Includes working papers documenting the administration of other committees and bodies, inter-governmental (both State/Territory and overseas) or inter-agency committees and bodies as well as groups set up to study issues and exchange ideas. Also includes documenting of: • management of committees, boards, working parties, working groups and task forces; • establishment, appointment of members; • terms of reference; • proceedings; • minutes of meetings; • agenda and reports; • arrangement or attendance at conferences and seminars; and • registrations, publicity and reports of participants incorporating: ▪ delivering presentations for professional associations; ▪ public relations; ▪ policy or program promotion; ▪ addresses and speeches; and ▪ lectures, briefs and multi-media presentations.	Destroy 6 years after actions completed

INFORMATION SECURITY

Entry	Description of records	Disposal action
20116	Records documenting the certification and accreditation (compliance) of information systems and products in accordance with Australian Government Information and Communication Technology Security Instructions (also known as ACSI). *Excludes records identified as Retain as National Archives.* Includes: • certification inspection reports; • assessing and reviewing system security documentation and management including issuing: • provisional certification; • withdrawal of certification; • auditing of government agency's systems; and • monitoring reports. *Note: Re-certification normally occurs on all certified gateways at least every 12 months or at initiation of a major change.* *Note: Provisional certification may be granted if the system is lacking compliance in some non-critical aspects of design, policy or management. It is issued to indicate that full certification can be expected, subject to successful completion of the provisions identified in the certification report. Failure to meet the provisions within the specified timeframe SHOULD result in provisional certification being withdrawn.*	Destroy 5 years after action completed

INFORMATION SECURITY

Entry	Description of records	Disposal action
20117	Administrative and operational records documenting the activities associated with marketing and industry liaison and Key management of the Information Security business. *Excludes records identified as Retain as National Archives.* Records include: • National Authority records documenting the marketing arrangements and liaison with clients and others to provide and receive information regarding the nature of output of the Information Security business. The activities may be carried out through direct contact and/or customer surveys and can involve: ▪ establishing priorities and requirements for Information Security; and ▪ seeking feedback on the content, presentation and distribution of National Authority products and support services. • National Authority and the Defence Cryptographic Controlling Authority records documenting: ▪ managing client accounts; ▪ approvals; ▪ procurement; ▪ production; ▪ maintenance; ▪ installation; ▪ distribution; ▪ disposal of keying material; and ▪ access to Communication Security (COMSEC) or cryptographic material/equipment, including • granting access to information systems, equipment; and • documentation to authorised users. • Defence Cryptographic Controlling Authority records relating to minor advice and routine operational matters including: ▪ High Grade Cryptographic Equipment (HGCE) system management; ▪ Communication Security (COMSEC) custodial appointments; ▪ procedures/instructions/reports relating to operations and exercises; ▪ COMSEC training; • physical security of ADF COMSEC facilities	Destroy 5 years after action completed

INFORMATION SECURITY

Entry	Description of records	Disposal action
20118	The Australian Defence Force (ADF) Communication Security (COMSEC) facility administrative and operational records documenting the activities associated with Key management of the Information Security business. *Excludes records identified as Retain as National Archives.* Records include: • access to COMSEC or cryptographic material/equipment; • granting access to information systems, equipment and documentation to authorised users; • copies of briefing/debriefing certificates; • development of keying material requirements; • use and management of keying material and associated hardware; such as: ▪ Accountable Classified Cryptographic Material (ACCM) accounting documentation including issue and receipts; ▪ ACCM muster, register, transfer and destruction records; ▪ COMSEC equipment accounting documentation including issue and receipt records; ▪ COMSEC equipment installations; • the ADF COMSEC facility records documenting/reporting incidents; • COMSEC audits; and • training activities.	Destroy 2 years after action completed
20119	National Authority and the Defence Cryptographic Controlling Authority records documenting inspections/audits of agencies/organisations/ADF Communication Security Facilities. *Excludes records identified as Retain as National Archives.* Includes: • certification of inspections reports; • monitoring reports including monitoring in support of exercises and operations; • countermeasure test results; and • COMSEC Audit reports.	Destroy 5 years after action completed