# ACSI 33
# Changes in the September 2004 Release

## Overview

**Introduction**

The *Australian Government Information Technology Security Manual*, also known as *ACSI 33*, was first released in its current form in March 2004.

This document covers the changes made to *ACSI 33* in the September 2004 release. It only identifies the changes from the most recent previous release.

**Not included**

The following types of amendments have **not** been noted in this document:

- typographical corrections,
- changes to the Index, and
- additions to the Abbreviations section.

**Versions**

Two versions of this document have been produced, one at UNCLASSIFIED, the other at SECURITY-IN-CONFIDENCE, consistent with the two versions of *ACSI 33*.

Changes that apply only to the SECURITY-IN-CONFIDENCE version of *ACSI 33* will be included only in the SECURITY-IN-CONFIDENCE version of this document.

**Terminology**

When referring to information within *ACSI 33*, the following definitions are used:

- **version** refers to the classification of the document, either UNCLASSIFIED or SECURITY-IN-CONFIDENCE,
- **release** refers to the month and year it was published,
- **part** refers to Part 1, 2 or 3 within *ACSI 33*, and is indicated by the part number followed by a dash, and
- **block** refers to the set of information delineated by horizontal lines within the document, and is denoted by a three digit number.

Within this document, blocks are referred to by their part number, followed by the block number.

**Example:** Block 430 within Part 3 is referred to as 3-430.

**Note:** Page numbers are not referenced, as they may not be consistent between versions or releases.

*Continued on next page*

## Overview, Continued

**Feedback**

Numerous comments and suggestions relating to *ACSI 33* have been received. Some of the changes noted in this document are a direct result of this feedback. Many other comments will require more time to resolve effectively, and the results will be seen in future releases.

Feedback on this latest release of *ACSI 33*, and on the format and/or content of this document, is also encouraged.

Contact details are in *ACSI 33*, Part 2, Block 105.

**Contents**

This document contains the following topics:

| Topic | See Page |
|---|---|
| Summary of Significant Changes | 3 |
| Listing of Minor Changes | 5 |
| Listing of Changed Blocks | 7 |

# Summary of Significant Changes

**Introduction**

The following blocks summarise the most significant changes included in the September 2004 release of *ACSI 33*. More detail on these changes is given in the last section, ‘Listing of Changed Blocks’.

**Document classification**

The minimum classification for IT security documentation for PUBLIC DOMAIN and UNCLASSIFIED systems has been reduced to UNCLASSIFIED.

**Block reference:** 2-219.

**Assessing the suitability of a DAP**

Added the product’s entry on DSD's EPL to the list of sources of information when assessing a DAP for its suitability.

**Block reference:** 3-311.

**Disposal of TEMPEST rated equipment**

Guidance on the disposal of TEMPEST-rated equipment has been added.

**Block reference:** 3-320.1.

**Labelling of High Grade Equipment and High Grade Cryptographic Equipment**

Policy on the labelling of High Grade Equipment (HGE) and High Grade Cryptographic Equipment (HGCE) has been added.

HGE **MUST NOT** have any non-essential labels applied to external surfaces.

HGCE **MUST NOT** have **any** labels applied to external surfaces without DSD authorisation.

**Block reference:** 3-413.1.

**Magnetic media sanitisation products**

Added an exception allowing non-DSD Approved Products to be used for formatting.

**Block reference:** 3-428.

**Fibre optic cables sharing a common conduit**

Added a new block that covers the application of Block 3-815 to fibre optic cables.

**Block reference:** 3-815.2.

*Continued on next page*

## Summary of Significant Changes, Continued

**Using DSD Approved Cryptographic Protocols**

The second paragraph of the block has been removed as it was causing confusion and a new dot point has been added to the first paragraph that refers the readers back to the minimum requirements tables.

The block title was also changed to be more relevant.

**Block reference:** 3-848.

**FIPS 140 updates**

Deleted the second paragraph of Block 3-858.

Added Block 3-859.1, which explicitly states that both 140-1 and 140-2 validations may be accepted.

Deleted Block 3-861.

Modified Block 3-862 to apply to evaluations at all EALs.

**Block reference:** 3-858, 3-859.1, 3-861, 3-862.

**Virtual LAN (VLAN) policy added**

The policy on the use of VLANs for network separation has been added.

**Block reference:** 3-947.1 - 3-947.5.

# Listing of Minor Changes

**Introduction**

This section lists those changes considered to have only minor impact on users of *ACSI 33*.

**NOIE / AGIMO amendment**

The reference to NOIE was replaced with AGIMO.

**Block reference:** 2-106.

**SOPs amendment**

Added "those relating to the roles of" to the sentences to improve accuracy.

**Block reference:** 2-115, 2-121.

**Added a definition for Server Room**

A server room has been defined as “a space containing servers and any associated communications equipment.”

**Block reference:** 3-116.2.

**DAP / DACP amendment**

Changed the "See:" to refer to the Cryptographic Protocols section, to explain what a 'correct implementation' is.

**Block reference:** 3-308.

**PEDs - related topics added**

Added references to the Infrared and Wireless sections to the table.

**Block reference:** 3-438.

**Separate audit log server**

Added a Note **RECOMMENDING** that systems be configured to save audit logs to a separate, secure log server.

**Block reference:** 3-709.

**Reference to AS/NZS 3080 added**

Added a reference to "AS/NZS 3080:2000 Telecommunications installations - Generic cabling for commercial premises".

**Block reference:** 3-807.

**DSD Approved Cryptographic Algorithms**

Replaced 'is “DSD approved”' with 'is a DSD Approved Product'.

**Block reference:** 3-843.

*Continued on next page*

# Listing of Minor Changes, Continued

**Incorrect AES key length**

The 196-bit AES key length was incorrect and has been replaced with 192.

**Block reference:** 3-846.

**DSD Approved Cryptographic Protocols amendment**

Replaced "approved protocols" with "DSD Approved Cryptographic Protocols".

**Block reference:** 3-849.

**Cordless and mobile phones**

Added a "See" after dot-point a. to Cryptography and DSD Approved Products.

**Block reference:** 3-885.

**Disposing of TEMPEST rated products**

Added a reference to the "Disposing of Products" section in Chapter 3 of Part 3.

**Block reference:** 3-898.

**Remote access standards**

Added in a "See" for dot-point d. to Physical Security and Cryptography.

**Block reference:** 3-940.

**Other minor changes**

Various other minor changes have been made to some blocks to improve the readability, accuracy or consistency of the document. These changes have no impact on policy.

**Blocks affected:** 1-109, 2-818, 3-112, 3-320, 3-509, 3-923.

# Listing of Changed Blocks

**Introduction**

This section lists all the blocks that have been added, deleted, or significantly amended.

**Deleted blocks**

Deleted blocks are indicated within the September 2004 release by a block label. The block text has been replaced with "<deleted>", and the block number is retained.

**Blocks affected:** 3-861.

**Added blocks**

All added blocks have been copied in their entirety (not including unchanged tables) into this section. Added blocks are indicated by a block number that includes a period followed by another number.

**Example:** 2-220.1 indicates a new block inserted after block 2-220.

**Format**

From this point onward, all blocks are presented as they appear in the September 2004 release, with following exceptions:

- any text within an existing block which has been added or amended has been highlighted,
- any unchanged tables within a block have not been shown,
- where information has been deleted, this is indicated by strike-through text, and
- the block number has been prefixed with the part number.

**Other organisations**

2-106. The table below contains a brief description of some of the other organisations that have a role in the security of Government systems.

| Organisation | Services |
|---|---|
| Australian Government Information Management Office ~~National Office of the Information Economy~~ | Development, coordination and oversight of Government policy on electronic commerce, online services and the Internet.<br>**URL:** http://www.agimo.gov.au/ ~~http://www.noie.gov.au~~ |

*Continued on next page*

**SOPs**

2-115. The ITSA **SHOULD** be familiar with all SOPs relating to the operation of the system, including those relating to the roles of the:

- ITSA,
- System Manager,
- System Administrator, and
- System Users.

**SOPs**

2-121. The System Manager **SHOULD** be familiar with all SOPs relating to the operation of the system, including those relating to the roles of the:

a. ITSA,
b. System Manager,
c. System Administrator, and
d. System Users.

**Document classification**

2-219. Agencies **SHOULD** apply the following classifications, as a minimum, to IT security documentation.

**Exception:** Agencies **SHOULD** classify security documentation that contains specific security configuration details at the level of the system to which it refers.

| System classification | Documentation classification |
|---|---|
| • PUBLIC DOMAIN,<br>• UNCLASSIFIED | UNCLASSIFIED |
| ~~• PUBLIC DOMAIN,~~<br>~~• UNCLASSIFIED~~<br>• IN-CONFIDENCE,<br>• PROTECTED | SECURITY-IN-CONFIDENCE |

*Continued on next page*

**Introduction**

3-101. Table 7.62 in Part E of the *PSM* sets out the minimum standard of security container or secure room required for the handling and storage of security classified information within Australia. This table is directed towards the storage of hardcopy material, and is not directly applicable to IT systems.

The purpose of this chapter is to:

- define physical security standards for IT systems, including communications equipment, servers and workstations, and
- assist agencies in developing an appropriate security environment for their IT systems that would meet the guidelines and established minimum standards of the *PSM*.

**The basics**

3-112. The basics of the physical security for an IT facility consist of:

- a perimeter enclosing the entire user network,
- a more restrictive area separated from general user areas containing the servers and communications equipment, and
- the protection of the facility by appropriate physical security measures.

The measures applied to the area containing the servers and communications equipment ~~server room~~ are designed to limit access to those with the authorisation and requirement to enter, and to detect those attempting to gain unauthorised access.

**Definition: Server Room**

3-116.2. A server room is a space containing servers and any associated communications equipment.

**Policy**

3-308. Agencies **SHOULD** use a DAP when they are relying on the product to enforce security functionality for the protection of classified Australian Government information and systems.

However, agencies **MUST** use either a DAP or a product that correctly implements a DSD Approved Cryptographic Protocol if the product contains cryptography that is used to enforce security functionality for the protection of classified Australian Government information and systems.
**See:** ‘DSD Approved Cryptographic Protocols’ on page 3-xxx for further information on the correct implementation of approved protocols. ~~DSD approval of cryptographic products on page 3-86.~~

*Continued on next page*

**Assessing the suitability of DAPs**

3-311. In assessing a DAP for its suitability to meet the security objectives of the agency, the agency **SHOULD** review the product's Security Target (ST) and Certification Report (CR) or similar documents, and any caveats contained in the product's entry on DSD's EPL, for the following:

a. its applicability to the intended environment,
b. that the version and configuration of the product matches that of the evaluated product,
c. that the required functionality was evaluated and certified,
d. that the level of assurance is adequate for its needs, and
e. for any constraints or caveats DSD may have placed on the product's implementation and use.

**Note:** Products that are in evaluation will not have a CR and may not have a published ST.

**TEMPEST rated equipment**

3-320.1. Agencies **SHOULD**:

a. reuse the equipment within the agency, or
b. offer the equipment to another Australian Government agency for reuse.

Agencies **MUST** contact DSD for advice if:
a. the above are unsuccessful, or
b. the equipment is non-functional.

**Labelling of High Grade Equipment and High Grade Cryptographic Equipment**

3-413.1. In order to maintain their tamper-evident design, HGE **MUST NOT** have any non-essential labels applied to external surfaces.

HGCE **MUST NOT** have **any** labels applied to external surfaces without DSD authorisation.
**Important:** This overrules any other labelling requirements stated elsewhere within this Manual.

**Magnetic media sanitisation products**

3-428. Agencies **SHOULD** use a DAP for the sanitisation of magnetic media.

**See:** 'DSD Approved Products' on page 3-xxx.

**Exception:** This does not apply to software used to format media in cases where the formatting of media is allowed as a means of sanitisation.

*Continued on next page*

**Audit trail protection and archival**

3-709. Audit logs **MUST** be:

a. protected from modification and unauthorised access,
**Note:** DSD **RECOMMENDS** that systems be configured to save audit logs to a separate, secure log server.

b. archived using a well-documented procedure and retained for future access, and
**Note:** DSD **RECOMMENDS** archiving audit trail data onto write-once media.

c. protected from whole or partial loss within the defined retention period.

**Important:** The retention of audit logs may be subject to the *Archives Act 1983*.

**Cabling standards**

3-807. Agencies **MUST** install all cabling in accordance with the relevant Australian Standards.

**References:**

- *Telecommunications Act (1997)*
- *AS/ACIF S009:2001 Installation Requirements for Customer Cabling (Wiring Rules).*
- *AS/NZS 3080:2000 Telecommunications installations - Generic cabling for commercial premises*

**Cables sharing a common conduit**

3-815. The table below shows the combinations of cable classifications that are approved by DSD to share a common conduit.

Agencies **MUST NOT** deviate from these approved combinations.

| Group | Approved combination |
|---|---|
| 1. | any combination of:<br>• PUBLIC DOMAIN,<br>• UNCLASSIFIED,<br>• IN-CONFIDENCE,<br>• PROTECTED,<br>• HIGHLY PROTECTED, and<br>• RESTRICTED. |

*Continued on next page*

**Fibre optic cables sharing a common conduit**

3-815.2. With optical fibre cables, the cable's protective sheath can be considered to be a conduit and therefore the fibres within the sheath **MUST** only carry a single Group.
**See:** 'Cables sharing a common conduit' on page 3-xxx.

If a cable contains subunits, as shown in Figure 4 below, then each subunit **MUST** only carry a single Group however each subunit within the cable may carry a different Group.

**Example:** the cable shown in Figure 4 could carry UNCLASSIFIED and HIGHLY PROTECTED in one subunit and CONFIDENTIAL and SECRET in another subunit.

The diagrams below represent a sample of fibre cross-sections.

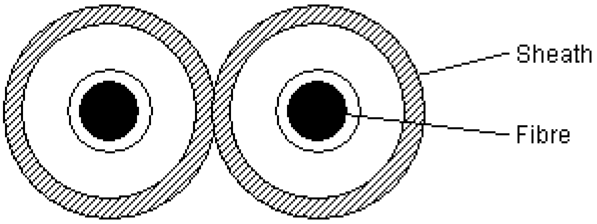

**Figure 1**

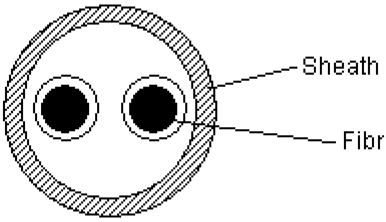

**Figure 2**

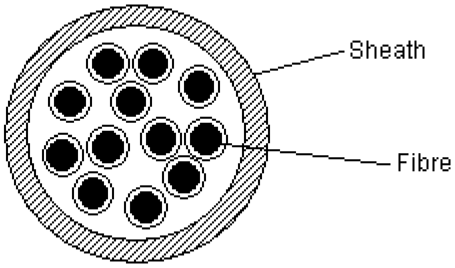

**Figure 3**

*Continued on next page*

**Fibre optic cables sharing a common conduit** (continued)

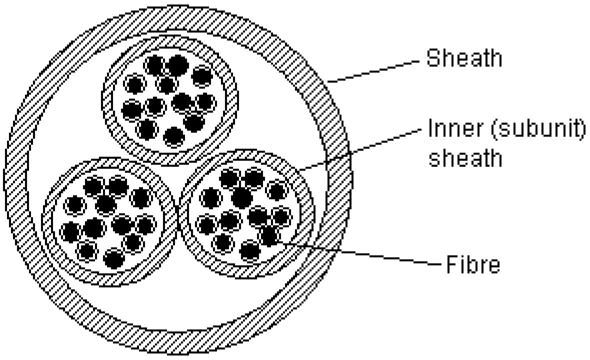

**Figure 4**

**Introduction**

3-843. This section explains the cryptographic algorithms that DSD has approved for the protection of non-national security classified information and RESTRICTED information. There are three types of algorithms:

- asymmetric/public key algorithms,
- hashing algorithms, and
- symmetric encryption algorithms.

**Important:** The fact that a product uses one or more of these algorithms does not automatically mean that the product is a DSD Approved Product. ~~"DSD approved".~~

**Using DSD Approved Cryptographic Protocols** ~~**Using evaluated products**~~

3-848. Before using an unevaluated product that implements a DSD Approved Cryptographic Protocol, agencies **MUST**:

a. investigate DSD Approved Products, and systems such as Fedlink, that provide greater security assurance,
b. ensure that the minimum requirements as stated in the 'Cryptography' section on page 3-xxx will be met, and
c. consider the risks.

~~Agencies **MUST NOT** use these protocols to transmit or store information on a network of a lower classification:~~
~~a. national security classified information classified CONFIDENTIAL, and above, or~~
b. ~~CABINET-IN-CONFIDENCE information.~~

**Links**

3-849. The table below lists the DSD Approved Cryptographic Protocols ~~approved protocols~~ and provides links to the relevant guidelines.

*Continued on next page*

**What is FIPS 140?**

3-858. The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of cryptographic modules, both hardware and software.

~~FIPS 140, formerly referred to as FIPS 140-2, is in its second iteration. For the purpose of this document, the standard is referred to as FIPS 140.~~

**Versions of FIPS 140**

3-859.1. FIPS 140 is in its second iteration and is formally referred to as FIPS 140-2. This policy refers to the standard as FIPS 140 but applies to both FIPS 140-1 and FIPS 140-2.

**Policy for cryptographic evaluations**

3-862. Cryptographic evaluations of products ~~at higher evaluation levels~~ will normally be conducted by DSD. Where a product's cryptographic functionality has been validated under FIPS 140, DSD may, at its discretion and in consultation with the vendor, reduce the scope of a DSD cryptographic evaluation ~~of a product validated under FIPS 140~~.

~~If the cryptographic functionality is validated under FIPS 140 then~~ DSD will review the FIPS 140 validation report to confirm compliance with Australia's national cryptographic policy.

**Note:** This policy also applies to products evaluated ~~to EAL2~~ overseas and submitted to the AISEP for Mutual Recognition.

**Cordless and mobile phones**

3-885. Cordless and mobile phones **MUST NOT** be:

a. used for classified conversations unless the security they use has been approved by DSD,
**See:** 'Cryptography' on page 3-xxx and 'DSD Approved Products' on page 3-xxx
b. connected to a classified telephone system, or
c. used in conjunction with a Speakeasy.

*Continued on next page*

**Standards**

3-940. Agencies that allow users remote access to systems containing classified information **MUST** ensure that:

a. the users are authenticated at the start of each session,
**Note:** DSD **RECOMMENDS** that agencies use more stringent measures to authenticate remote users than it would for users accessing the systems from sites under the physical control of the agency.
b. the users are given the minimum system access necessary to perform their duties,
**Note:** DSD **RECOMMENDS** that agencies do not allow the use of privileged access remotely.
c. the users can only access the agency's system from systems accredited to at least the classification of the agency's system, and
d. any data transferred is appropriately protected during transmission and at the remote user's end.
**See:** 'Chapter 1 - Physical Security' on page 3-xxx and 'Cryptography' on page 3-xxx.

**Introduction**

3-947.1. Many Layer 2 switches can provide a Virtual LAN (VLAN) capability that allows:

a. multiple Layer 3 networks to exist separately on a switch; and
b. a network of computers to behave as if they are connected to the same wire even though they may actually be physically located on different segments of the LAN.

**Important:** The VLAN capability within switches is not designed to enforce security and a number of techniques have been documented that may allow traffic to pass between the VLANs.

*Continued on next page*

**Connectivity policy**

3-947.2. The table below represents the connectivity policy for VLAN networks sharing a common switch:

Key:

| **Level** | **Policy** |
|---|---|
| A | DSD does **NOT RECOMMEND** |
| B | Agencies **SHOULD NOT** |
| C | Agencies **MUST NOT** |

| | **PD** | **U** | **IC** | **R** | **P** |
|---|---|---|---|---|---|
| **PD** | A | B | C | C | C |
| **U** | B | A | B | C | C |
| **IC** | C | B | A | B | B |
| **R** | C | C | B | A | C |
| **P** | C | C | B | C | A |

**Configuration and administration policy**

3-947.3. Administrative access **MUST** only be permitted from the most highly classified network or, for networks of the same classification, the most trusted network as determined by the Accreditation Authority.

Staff with administrative access or unsupervised physical access to the switch **MUST** have a security clearance of at least the classification of the highest classified network carried on the switch.

The physical security of the switch **MUST** meet the requirements for the highest classified network carried on the switch.

Agencies **SHOULD** implement all security measures recommended by the vendor of the switch.
**Note:** If any of the recommendations conflict with ACSI 33 then ACSI 33 has precedence.

Unused ports on the switches **SHOULD** be disabled.

**Trunking**

3-947.5. Using a technique known as trunking, a VLAN may exist across two or more connected switches.

This capability **MUST NOT** be used on switches managing VLANs of differing classifications.