Defence Signals Directorate
Information Security Policy Advice 1/2003

Recognition of FIPS 140

Date of Effect: 10 December 2003

Information Security Group
Locked Bag 5076
KINGSTON ACT 2604
AUSTRALIA

Ph: (02) 6265 0197
Fax: (02) 6265 0328

assist@dsd.gov.au
www.dsd.gov.au/infosec

RECOGNITION OF FIPS 140

Introduction

What is FIPS 140?

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

At the time of promulgating this policy, FIPS 140 is in its second iteration (formally referred to as FIPS 140-2). For the purpose of this document, the standard is referred to as FIPS 140.

What FIPS 140 is not

FIPS 140 is **not** a substitute for the evaluation of IT security products under the Common Criteria. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other information security functionality.

For more information on FIPS 140

See: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Policy

General policy regarding cryptography

The Commonwealth *Protective Security Manual* (PSM) states that "all measures using cryptography to protect Commonwealth information must be approved by DSD and must be implemented in accordance with DSD guidelines." (PSM C5.15)

Policy for cryptographic evaluations at the EAL2 level

Vendors entering products into the Australasian Information Security Evaluation Program (AISEP) for evaluation at EAL2 may, at their discretion, choose to have the product's cryptographic functionality evaluated by DSD, or validated under FIPS 140.

If the cryptographic functionality is validated under FIPS 140 then DSD will review the 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.

Continued on next page

Policy, Continued

Policy for cryptographic evaluations at all other levels

Cryptographic evaluations of products at higher evaluation assurance levels will normally be conducted by DSD. DSD may, at its discretion and in consultation with the vendor, reduce the scope of a DSD cryptographic evaluation of a product that has been validated under FIPS 140.

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

Note: this policy also applies to products evaluated overseas and submitted to the AISEP for Mutual Recognition.

Approved algorithms

Some algorithms approved for use under FIPS 140 are not currently approved by DSD for the protection of classified Australian Government information.

Modules that have been FIPS 140 validated, but do not include any DSD-approved algorithms in the validation, will **not** be approved by DSD for the protection of classified Australian Government information.

See Australian Communications-Electronic Security Instruction (ACSI) 33 for more information on the DSD-approved algorithms.