Australian Government
Department of Defence
Defence Export Control Office

Telecommunication and Information Security Goods

Classification Guide

Purpose

The purpose of this document is to describe the decision making process used by DECO to classify telecommunication and information security goods, including radios, listed in the Defence and Strategic Goods List (DSGL).

Background

The following definitions are given in the preface of the DSGL:

Military goods are those goods or technologies that are designed or adapted for military purposes including parts and accessories thereof.

Dual-use goods comprise equipment and technologies developed to meet commercial needs but which may be used either as military components or for the development or production of military systems or weapons of mass destruction.

The classification of telecommunication and information security goods, including radios, can be challenging. The primary reason for this is the rapid technological development of these fields. It is not unusual that commercial requirements for these technologies equal or exceed those of military applications. Companies often develop products that are advertised for different markets (commercial and military) with very little or no differences between them. The purpose of export controls is to ensure that products are subject to control based on the functionality that is present, rather than on any specific marketing or design that is intended to make the items appear to be non-military. It is not uncommon that military users choose COTS (commercial off-the-shelf) components when they can achieve the required performance levels, especially when they are working within a restricted budget.

Overview of the controls

Part 1 of the DSGL controls all electronics, *specially designed for military use*, under item ML11.a. The item has a non-exhaustive illustrative list of included items, but does not have any decontrol guidelines or technical notes that limit the extent of the control.

Part 2 of the DSGL controls telecommunication equipment under item 5A001 while information security systems, equipment and components are controlled under item 5A002. Many telecommunication and information security goods exported from Australia, especially radios, contain features that meet the requirement of one or both of these sections. Common features include digital encryption, frequency hopping, low-rate voice encoders and EAL6+ evaluation.

Classification of items

Items can be controlled as either military or dual-use items. If an item could fit into both categories, it will be classified as a military item. The following four-step process is used to assess all telecommunication and information security items, including radios:

1. Any item with a feature in Table 1 will be classified as a military item.
2. Any item with a feature in Table 2 will be classified as a dual-use item.
3. Any dual-use item with at least one indicator from Table 3 will be classified as a military item.
4. Any other item with at least three indicators from Table 3 will be classified as a military item.

Table 1: Military Features

Item can be fitted to military equipment only, e.g. it uses mechanical, electrical or optical interfaces that are not used in commercial communication equipment Note 1
Development of the item is sponsored by military forces Note 2
Item has a Joint Electronics Type Designation (JETDS) or any other special military equipment designation number Note 3
Item is certified or designed for any part of MIL-STD-188 (or relevant STANAG communication standards) that does not have a commercial equivalent – not including MIL-STD-188 subsections 110A/B or 141B Note 4

Table 2: Dual Use Features

Feature	DSGL reference
Special EMP / radiation / temperature hardening	5A001.a
High capacity radio transmitters	5A001.b.2
Spread spectrum / frequency hopping	5A001.b.3
Ultra-wideband modulation	5A001.b.4
High capacity digitally controlled radio receivers	5A001.b.5
Voice coding at rates of less than 2400 bit/s	5A001.b.6
Radio direction finding equipment >30MHz	5A001.e
Jamming equipment for mobile telecommunication services	5A001.f
IP network communications surveillance systems	5A001.j
Digital cryptography	5A002.a.1
Cryptanalytic functions	5A002.a.2
Designed to reduce compromising emanations (TEMPEST)	5A002.a.4
Cryptographic spread spectrum / frequency hopping	5A002.a.5
Cryptographic ultra-wideband modulation systems	5A002.a.6
Evaluated to assurance level exceeding EAL-6	5A002.a.7
Quantum cryptography	5A002.a.9

Table 3: Indicators for Military Equipment

Certified or designed to military environmental standards such as MIL-STD-810 Note 5
Certified or designed for military EMI susceptibility standard such as MIL-STD-461 Note 6
Designed to reduce the probability of detection, interception or jamming (other than those features that are controlled on the Dual Use List), including encryption in any form Note 7
Designed as a 'manpack' radio Note 8

Notes

The following notes clarify the descriptors in Tables 1 and 3 above. The descriptors in Table 2 require no further clarification, as they are drawn directly from the DSGL.

1. Items with specifically designed interfaces that can fit only on military equipment are, by definition, designed for military use only. Interfaces in this context are: mechanical mounting brackets; electrical connectors; computer hardware/software communication standards and similar.

2. Items sponsored by defence/military forces and/or associated agencies are often of high technological sensitivity and always designed for military use with specifically defined interfaces and functionalities.

3. Joint Electronics Type Designation System (JETDS) is a US designation system for military electronics. JETDS is described in detail by MIL-STD-196. It is commonly known as the 'AN' system.

4. MIL-STD-188 is a family of US military standards that cover military communication equipment and protocols. Some of the standards in this family have Federal Standard (FED-STD) counterparts that pertain to commercial telecommunication equipment, which are therefore not covered in Table 1. The control specifically excludes subsections 110A/B (data modems) and 141B (ALE) due to their widespread use in civil systems.

5. MIL-STD-810 standard (the latest revision is G but the F revision is still in use) is a set of environmental specifications that military equipment has to be designed for. This standard is most commonly used for testing the equipment and certifying the operational temperature/humidity and shock/vibration conditions that the equipment is designed for. No equipment can pass the entire suite of tests described in this standard since it is tailored for various environments (land, air and sea) and a specific list of tests has to be chosen depending on the end-use of the equipment.

6. EMI (electromagnetic interference) susceptibility is a design factor for both civil and military radios and telecommunication equipment. The control focuses only on those goods designed and/or certified to the relevant military standard.

7. This control is looking at functionality that is not specifically listed in the DSGL (see features in Table 2) but is a capability of the equipment (whether operating or not). This includes:

    a. Spread-spectrum techniques, including with a fixed sequence

    b. Burst transmission, including with a fixed sequence (not including those 'burst' elements of ALE protocols)

Notes continued

c. Controlled reception pattern antennae

d. Analogue voice scramblers

e. Power management for reduced probability of intercept

8. A ‘manpack’ radio is a high-power radio designed to be carried by an individual on foot. ‘Manpack’ radios may have greater military utility than vehicle-mounted or base station radios because they can be deployed with military or paramilitary forces in any terrain as part of infantry operations. In this context, the term ‘manpack’ does not include low-power short range VHF handheld radios, but does include backpack-mounted HF radios.

9. Cryptography that only performs the functions of authentication, digital signature or execution of copy-protected software is not considered to be 'digital cryptography' listed in 5A002.a.1, or 'a feature that is designed to reduce the probability of detection, interception or jamming' listed in Table 3. This specifically includes general-purpose hardware that uses cryptography to decrypt its own firmware, where that cryptography has no other function. The actual content/functionality of the firmware itself may still be subject to export control.

Controls on Test, Inspection and Production Equipment, Software and Technology

Although not discussed in detail in this document, there are controls on:

- 5B001 – Telecommunications test, inspection and production equipment
- 5D001 – Software
- 5E001 & 5E101 – Technology
- 5B002 – Information security test, inspection and production equipment
- 5D002 – Software
- 5E002 – Technology

Where can I get more information?

You can access the Online DSGL Tool at https://dsgl.defence.gov.au for further information on the controls. If you are still unsure if your goods are controlled for export, you should seek advice from DECO.

More information on the export controls administered by DECO as well as the application forms required to apply for a permit can be found at www.defence.gov.au/deco

Email: deco@defence.gov.au

Phone: 1800 66 10 66