

# The CPNI PRODUCT RATING SYSTEM

## A GUIDANCE DOCUMENT

December 2016

**Disclaimer:**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

The text of this publication may not be reproduced, nor may talks or lectures based on material contained within the document be given, without written consent from the Centre for the Protection of National Infrastructure (CPNI).

## Contents

**Aim**..... 2

**Background**..... 2

**What does CLASS mean?** ..... 2

**What is PROTECTION Level?** ..... 3

**Can a product achieve both?**..... 4

**Summary**..... 5

**Further Reading** ..... 5

## Aim

The aim of this document is to provide guidance to help distinguish the difference between Counter Espionage (CE) and Counter Terrorism (CT) grading and to help you decide which products you require for a given application, based on a number of factors such as threat, risk and the operational requirement.

## Background

CPNI evaluate security products for use in the CNI and Government. These evaluations are undertaken by contracted test houses who are competent in the evaluation of these products. Upon completion CPNI convenes a panel of experts to assess the results of the evaluation. After careful consideration of the written report, and other factors, successful products are awarded a grading. This grading may be either a CLASS level or a PROTECTION Level or both. It must be stressed that CPNI are assessing products for use in **high security** environments. As a result, the evaluations carried out are well above the standard expected of a ‘normal’ security product. Relatively few products pass, so even the ‘lowest’ CPNI grading still points to a very capable product.

## What does CLASS mean?

The CPNI CLASS rating is given to a product that has characteristics that will defend against surreptitious attack. This is the kind of attack which will be carried out by a party who wishes to gain access to classified material for nefarious reasons. It may be that the attacker wishes to steal information, deny service, install malicious software, etc. The important point is that the attacker would generally wish to go un-noticed. This means they will not want to leave any indication that an attack has taken place. **The emphasis of a CLASS product is Detection.** It is possible for a product to achieve a CLASS rating without providing any protection against forcible attack. However, it has to be said that CLASS without PROTECTION is probably an unlikely requirement. Obviously, we would prefer that the adversaries could not gain access to our secrets by stealth or forcible attack.

As the attacker does not want to get caught, for CLASS rated equipment the emphasis is on **detection of compromise or tamper indication**.

A CLASS attacker will often play the 'long game' and CLASS attackers will undertake an attack over many months or years (including reconnaissance, preparation and the attack). They may require repeated or long term access for this to happen.

It is possible to achieve a CLASS rating in a number of ways. Some examples are below:

- Make a product capable of auditing its use
- Make a product so that any interference will show signs (anti-tamper)
- Design a product such that an attack may be possible but a long time is required
- High level of detection or performance (e.g. very good alarm detection rates)

A CLASS rating will defend against **espionage**, be it state sponsored or industrial. Remember, the attacker does not wish to be discovered. For the owner of the product, the main aim of the product is to detect an attack so that remedial action can be taken. It must be remembered that given the correct resources and enough time everything can be overcome – a CLASS product will at least tell us when it has been compromised.

**CPNI grades for surreptitious attack are:-**

**CLASS 1 – CLASS 2 – CLASS 3 – CLASS 4 (highest)**

CPNI CLASS ratings are, by their very nature, not for public knowledge. As a result a company will not publicise their CLASS rating or the fact that a product has been given one. Similarly, the CLASS rating must not be transmitted by a non-government email system.

## What is PROTECTION Level?

The CPNI PROTECTION Level is given to a product which shows resistance to forced attack. This is based on the perceived skill level of the attacker and the time a product will resist that attack. It is assumed that the attacker is not concerned with leaving evidence of the attack. The only goal is to defeat the product and gain entry. This kind of attack is primarily associated with a **terrorist** threat. The actual goal of a terrorist being very different to the surreptitious attacker. In many cases the terrorist actively courts attention so they are not put off by the prospect of being discovered.

**CPNI grades for forced attack protection are:-**

**BASE – ENHANCED – HIGH.**

CPNI establish the grading based on trials and evaluations which indicate how long a product will delay an attacker of differing capabilities. The time delay is not common across all product types. For example a BASE fence will not give the same delay as a BASE door. For manual forced entry, CPNI qualify the grading with a time figure (e.g. BASE 5 minutes). Your CPNI advisor can help you with the details.

An attacker will want to achieve their end aim (destruction or theft of an asset) as fast as possible. **Therefore for PROTECTION Level equipment the emphasis is on Delay.**

It has already been said that many products fail to achieve a CPNI grading at all so a BASE product is a good product in its own right.

Remember – a ‘forced’ attack can take a number of guises. A forced attack against a door will look very different to a forced attack against an access control system. Ask your CPNI advisor for assistance if required.

## Can a product achieve both?

A number of CPNI evaluated products achieve both a CLASS **and** a PROTECTION level. This is because the product has shown resistance to both forms of attack. These products are suitable for many situations and provide a good solution if your site/establishment has both a CT and CE threat. Once again, it will be the threat and the operational requirement that will drive your product selection.

It was mentioned earlier that a combination of CLASS and PROTECTION measures will probably be required. It should go without saying that on many occasions, simply knowing about a loss may not be enough. We may need to prevent the loss of material (and if it is lost, then definitely be aware of the loss).

	CLASS	PROTECTION
<b>Speed</b>	May be slow Could take many months (but not necessarily)	As fast as possible
<b>Key principle</b>	Detection	Delay
	Possibly NO delay	Speed of response is important

A product which provides both CLASS and forced attack PROTECTION is an ideal solution. However, many products in the CSE will be rated in only one area. It will be necessary to use these products together in order to achieve the desired level of security. Layered security is key.

A very simple way of looking at things might be:

- CLASS products keep things in
- PROTECTION Level products keep people out

Combine the two to get the solution you require.

## Summary

CPNI evaluations are conducted in order that the CNI and Government can make an informed choice when selecting security products. The PROTECTION Level and CLASS gradings are the tools by which a site can make that informed choice. The type of product or the combination of products chosen will depend on the threat and be driven by the Operational Requirement. It is important that the right products are chosen for the job you want it to do.

## Remember...



## Further Reading

- Guide to Producing Operational Requirements for Security Measures and associated documents on the CPNI website and extranet
- CPNI Trademark Guidance document on the CPNI website and extranet