



NIAP Update



2005

National Information Assurance Partnership



CIMs

DOC


Consistency Instruction Manual

For development of

US Government Protection Profiles

For use in

Basic Robustness Environments



Information
Assurance
Directorate

Release 3.0

1 February 2005


Consistency Instruction Manual

For development of

US Government Protection Profiles

For use in

Medium Robustness Environments



Information
Assurance
Directorate

Release 3.0

1 February 2005

1

PP Validation

● Current Feedback

- Labs are intended to provide “checks and balances complementing validators and providing the project evaluation reports that are not written by the NIAP validators.
- It is likely that a lab would have to be engaged.

● NIAP’s PP group could take on the task of authoring “government” PP’s based on the IEEE PP’s.

- NSA customer advocates would first have to document customer need for the PP’s
- Organizations such as DAPS could make the request
- The government “High Security” PP would be consistent with the government definition of the term and would not be an EAL2 Profile

NIAP Feedback

- CC Version 3 will take a different approach to encryption
- International signers of the new agreement could require encryption implementations approved by a “national authority” in place of FIPS.
- No encryption will be “required” but will be described as desirable for data transit and storage.

NIAP Feedback

- The IEEE use of the term “High Security” in connection with an EAL2 Profile is misleading and could cause user confusion.

“I am confused with the "high security" name being used. All environments have a need for high assurance (security) functionality.

Even in the public environment there has to be admin functions or maintenance functions that need to have a high level of assurance and protection to ensure the Public does not bypass or corrupt the functionality of the device.”

NIAP Feedback

If "High Security" is equated with government why not call it Government Environment or another name mapped to the target. High security at EAL2 is confusing. Like I indicated, all environments, including government, need high, medium and basic robustness protections. The threats and/or policies usually lead the PP developer in selecting the appropriate robustness requirement in the PP. In fact you address this issue as Threat Risk level in Clause 7: Hardcopy Device Threats (8/9/05) on the technical doc page on the web site but not in the profile, why not. Functionality and assurance is dependent on the threats in the environment.

NIAP Feedback

You mentioned that you looked at the "NIAPs Basic Robustness Manual". I do not understand why you would not want to address the functional and assurance requirements (as a minimum) that are included in that document. Basic Robustness included functionality that should be included in all products that are security enabled and that functionality should be built to the assurance level described in the manual.

For basic robustness, the assurance level is EAL2 augmented with Flaw Remediation (ALC_FLR2) and Examination of Guidance (AVA_MSU.1). Basic robustness is not that difficult to achieve and the only thing unique to the US would be the augmented assurance requirements that could be achieved by any international scheme. By the way the current manual may have references to NIAP interpretation but they went away with the new CC version 3.0.

Why would you not address basic robustness as described in that manual?

NIAP Feedback

I reviewed the threats listed in the PP and the threats that you have listed on your web site at Clause 7: Hardcopy Device Threats (8/9/05) on the technical doc page and they do not seem to align in any way. How do these documents relate? When will the correct list of threats be addressed?

Map threat level to level of risk assessment.

NIAP Feedback Summary

- A lab may have to be engaged if the PP is to be validated.
- NIAP might generate “government” PPs based on the IEEE PPs
- Conform with the recommendations in the Robustness Manuals
- Follow Version 3
- Reconsider the use of the term “High Security” for the current profile
- Revisit the relationship of the threat list to the PP