Assurance Activity Reporting for Evaluations Against NIAP-Approved Protection Profiles

This paper updates a previously issued NIAP guide for Assurance Activity Reporting by including the effective date which was previously posted separately in a NIAP website Announcement. The contents of the AAR remain the same per earlier NIAP guidance.

This paper outlines the required content of Assurance Activity Reports (AARs), which are published in order to standardize publicly available information from evaluations against NIAP-Approved Protection Profiles and to promote consistency in the review and performance of those evaluations.

The goal of AARs is to provide system integrators with useful information about evaluated product testing and configuration, help to align Common Criteria evaluations with DISA Security Requirements Guides and Security Test Implementation Guides (SRGs/STIGs), and thereby streamline the process for U.S. Government procurement of validated products.

Additionally, standardized reporting will help NIAP revise and create more clear and objective assurance activities in the future while also supporting transparency and consistency among nations in the Common Criteria Recognition Arrangement.

While a format is suggested by this whitepaper, other formats that present the content indicated are acceptable. It should be noted that the focus of the evaluation effort is on the performance of the Assurance Activities, and thus this whitepaper focuses on the reporting documentation associated with those elements of the evaluation.

Effective Date

For each NDPP-compliant evaluation submitted after 1 January 2014 and all evaluations submitted after 1 April 2014, an AAR will be published on the NIAP Product Compliant List.

Applicability

While some discussion is centered on Network Device Protection Profile (NDPP) evaluations, the format, information, and overall intent is to perform the reporting described in this white paper for all evaluations against PPs that contain assurance activities. It may be the case that certain PPs will require more or less information to be presented in some areas, but these cases will be handled on as as-needed basis.

Assurance Activity Report

Assurance Activities in the PPs require three types of information: requirements on information contained in the TSS (and other supplemental documentation), requirements on information contained in the guidance (AGD) documentation, and testing requirements. For each SFR and SAR in the PPs, the associated Assurance Activities contain at least one of these categories of information, but potentially will not have all three types of actions (for example, some SFRs/SARs will just require documentation be present in the TSS, but will have no associated testing activity). For the assurance activity associated with each SFR, the AAR shall contain an indication (as detailed below) for each type of activity (TSS, Guidance, Test), or "none" if there is no activity. For example, the write-up for FIA_PMG_EXT.1 in the NDPP might look like:

> **TSS**
>
> None
>
> **Guidance**
>
> Guidance for the composition of passwords, as well as for setting parameters associated with passwords used for the local administrative connection, is contained in *FooBar 2000 Security Administrator's Guide* version 1.0, 21 June 2012.
>
> **Testing**
>
> *<test procedures—see below>*

The following sections outline more detailed presentation evidence for each of the above types Assurance Activities.

Reporting on TSS Assurance Activities

Information required to be in the TSS is largely self-documenting, meaning that the evaluator in most cases is required to ensure that it is present in the TSS, but little beyond that is required in most PPs. For most TSS assurance activities in the AAR, a simple indication that the information is present and a pointer to that information in the ST is sufficient; it is not required to copy and paste the assurance activity or the information in the TSS into the AAR. It is expected that the evaluator ensure that the information in the TSS as a whole is consistent, and that spurious information is not included.

For some information in the TSS, the evaluator may be required to make a judgment on that information relative to the security requirement being levied. For these requirements, the evaluator shall write up their rationale in the TSS section of the AAR.

Reporting on Guidance Assurance Activities

The AAR lists specifically all documents used—for each platform, model, and hardware component (chassis, blade, processor, etc.)—to satisfy the requirements for operational guidance assurance activities. Each applicable administrative manual must be identified in a manner such that an end user can locate the specific manual used for the evaluation. It is acceptable to list general manuals that have evaluation-specific addenda, as long as both are identified.

For each assurance activity referencing information in the operational guidance, the AAR must list—for each model that has a distinct manual or manuals—the specific manual that contains the information, along with a pointer to the section or sections that satisfy the requirement in the assurance activity.

Reporting on Test Assurance Activities

It is intended that the AAR be accessible on the NIAP web site—along with the ST and validation report—for the evaluation. While test information is required as outlined below, detailed test information does not have to be made available in the same manner as the ST. While the detailed information described below will have to be made available to the scheme (and potentially to other CCRA schemes as well), a summary will be sufficient for posting in the AAR along with the ST and validation report. The requirements for the detailed testing report are listed below, followed by the requirements for the summary.

It should be noted that it is acceptable to use developer-developed tests to satisfy the test assurance activities. There are several stipulations for their use, however:

1. The developer is not obligated to provide such test, nor are they obligated (if they provide tests) to put the tests in any particular format. The intent is that the developer provides what they normally use, not something produced specifically for the evaluation.
2. If developer tests are used, the evaluator must run or witness the tests. It is not sufficient for the developer to merely send test output to the evaluator.
3. Any additional documentation required with respect to the detailed or summary reporting (outlined in the following sections) concerning developer-supplied tests is the responsibility of the evaluation team.

Detailed Testing Information

The test information in the AAR consists primarily of a test report. While it is expected that the evaluation team will first prepare a test plan; execute that test plan; and produce a test report; the evidence presented to the valuation team in the AAR will contain all of that information and is referred to as a “test report” below.

The test report identifies the platforms to be tested, and for those platforms not included in the test report but included in the ST, the test report provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to

merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test report describes the composition (hardware, software, pluggable modules, etc.) of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of any cryptographic engine to be used.

The test report contains the test cases to be exercised by the evaluators; these can either be developer test cases or evaluator-developed test cases. These test cases address each of the "test" elements in the assurance activities in the PP, as well as any potential vulnerabilities to be tested as outlined in the AVA_VAN.1 assurance activity.

Each test case consists of a test objective, test configuration, test instructions, test steps, and test results. The test objective contains an abstract description of the test; this is generally the "test" assurance activity from the PP. It may be the case that elaboration of the objective is warranted after performing operations on the component, or due to the particular implementation of the component in the TOE. In these cases, a more relevant test objective may be crafted and included in the test report. The test configuration consists of any test setup that must be accomplished prior to the test in order for the test to successfully run. The test instructions contain information pertaining to running the test. For automated tests, this consists of the "run this test" instruction and any information pertaining to the output. For manual tests, the test instructions are usually identical to the test steps. The test steps contain the specific steps to be followed in performing the tests. For automated tests, this consists of the contents of the test script; this could be code, scripted command line instructions, test harness language programs, etc. For manual tests, this consists of the steps that the tester must perform in order to accomplish the test (e.g., command line commands; instructions on setting radio buttons, checkboxes, and filling in parameters on GUI-based interfaces). The test results consist of the expected results from running the test. These results are the effect that the test has on the TOE, as well as how this result is checked. For automated tests this is often located within the test steps themselves, with the visible result to the user being "test passed". In other cases (most often manual tests), some observation is made while performing the test steps.

The test report details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result. Additionally, any setup or configuration steps needed to ensure the test operates as planned must be included in the detailed test report.

It is intended that the information regarding testing in the AAR provide a clear picture of the TOE configuration used for testing and a reasonable reproduction of test instructions and results of individual tests. The level of detail of the test steps should be such that 1) it is clear that the instructions in the AGD guidance were sufficient for configuring the TOE for the test and 2) an independent (of the CCTL performing the testing) 3rd party has sufficient information to reproduce the tests as they were performed by the evaluators, including setup of the test configuration in terms of both the hardware and software used in the test.

Summary Testing Information

For the publically available (published) AAR, the specific test steps and associated detailed results do not need to be made available. Rather, a summary description of the test and results will be sufficient. For example, when testing the setup of an IPSEC connection, the detailed test case would contain all of the commands used to configure the connection and perform the test, as well as the detailed results (screenshots, packet dumps, etc.) of the test. The summary testing information, on the other hand, could contain high level statements such as "configure the SA" and "initiate the IPSEC connection" without referencing detailed commands or the output of those commands.

Initially, significant effort will be expended by NIAP (in conjunction with end users and evaluation facilities) to determine an appropriate level of summarization that allows end users to have relevant insight into how the mechanism was actually tested while protecting proprietary techniques and procedures developed by the evaluation facility to enhance testing efficiency and cost effectiveness.