Entropy Requirements in Network Device PP Evaluations

NIAP recognizes the requirements for entropy in the Network Device PP (NDPP) pose challenges for the community as no existing standard incorporates the specific requirements at this time. We understand that describing and analyzing entropy at this level of detail is a new requirement, but it is necessary to address weaknesses in our national security systems that impact the soundness of the cryptographic solutions. NIAP has a multi-phased approach to addressing the Random Bit Generation/Entropy requirements for NDPP compliant evaluations in the near term and beyond. NIAP strives to provide vendors and CCTLs with consistent and repeatable guidance now and tools in the future so the impact of these requirements will lessen as the community becomes more knowledgeable about the requirements and entropy in general.

Currently, the draft NIST publication 800-90B may be referenced as guidance for entropy implementations. The publication is not currently mandated by NIAP because it is still in draft form. However, this publication may be used as helpful guidance by vendors and CCTLs. When the publication is finalized, compliance to the standard will be incorporated as part of the NDPP requirements

Today, the goal for NIAP-approved PP compliant evaluations is to complete within 6 months. Therefore, prior to a product being included on the NIAP in-evaluation list, it is expected the product will have a security target that contains all the information required by the NDPP assurance activities. Further, the evaluation team is expected to perform a review to ensure all assurance activities can be completed in a timely manner. This review will include evaluation team confirmation that documentation of the entropy architecture in accordance with Annex D is adequate for completion of the RBG assurance activities. Note that there is no requirement for verdicts on Security Functional Requirements as part of the check-in package. Rather, the evaluators must have confidence that the information delivered by the vendor contains the appropriate level of detail to perform all assurance activities. Once the CCTL concurs the product is ready for evaluation per the evaluators' review, the ST, including documentation of the entropy architecture in accordance with Annex D, will be submitted to NIAP as part of the check-in package.

As part of NIAP validation oversight for entropy, and in assisting both CCTLs and vendors in familiarization with entropy validation, the Information Assurance Directorate (IAD) will provide NIAP validators support to ensure entropy analysis is complete and correct.

Upon successful review of the check-in package by NIAP, an evaluation check-in meeting will be held and the product will be added to the NIAP in-evaluation list. During the course of the evaluation, as soon as the evaluators have completed the RBG and Annex D requirements analysis and assurance activities, the results must be delivered to NIAP for validation oversight review.

NIAP is working to deliver an entropy test tool to our CCTLs in the future that will allow for testing of entropy implementations to enhance repeatability and streamline the entropy review process.

Until the tool is delivered and NIST SP 800-90B is finalized, NIAP will continue to share entropy lessons learned in order to promote consistency in NDPP evaluations.