28 March 2012

Frequently Asked Questions for NIAP/CCEVS and the Use of Common Criteria in the US

1. What transformations are occurring in NIAP?

Answer: NIAP is transforming Protection Profiles, evaluation methodologies, and policies to ensure Achievable, Repeatable, and Testable evaluations. Evaluation Assurance Levels (EALs) and Robustness will no longer be specified in NIAP evaluations.

NIAP approved Protection Profiles are being created for technologies of high priority for our U.S. customer base and the Commercial Solutions for Classified Program (http://www.nsa.gov/ia/business_research/ia_bao/commercial_solutions_for_classified_program.shtml). We are working with industry, our customers, and the Common Criteria community to form Technical Communities to create these PPs. The first generation Protection Profiles takes into account the current assurance that is achievable for a technology; and assurance activities are generated based on the availability of the documentation, test plans, and tools needed to obtain consistent and comparable results.

See the list of published NIAP Protection Profiles (http://www.niap-ccevs.org/evolution/pps) as well as those we are developing (http://www.niap-ccevs.org/pp/draft_pps).

As a result of more objective requirements in NIAP approved PPs, evaluation methodologies will be less subjective and thereby more consistent among Common Criteria Test Laboratories and across international CCRA Schemes.

NIAP Policies and Publications are currently being updated to reflect these changes.

2. Why is NIAP implementing these changes?

Answer: Based on over 10 years of experience with Common Criteria evaluations, the NIAP program has concluded consistent and repeatable evaluation results require a Protection Profile with tailored assurance activities developed in partnership with vendors and the other Common Criteria Schemes, defined as a Technical Community. The changes in policy are the natural result of understanding the assurance that can be achieved with different types of technologies and the limitations of what can be achieved through the evaluation of vendor products. Although EAL4 has become the defacto standard for evaluation, the generic EAL4 requirements are not relevant, achievable and repeatable in all cases. Given this false label of assurance, the creditability of NIAP and the Common Criteria in general has been negatively affected. To restore the CC brand, it is necessary to restrict evaluations to technology specific Protection Profiles with achievable, repeatable and testable requirements and assurance activities.

The rationale for change is as follows:

- Comparable, consistent evaluation results require an agreed upon threat model and set of security functional requirements that must be captured in a Protection Profile;
- Comparable, consistent evaluation results require documenting tailored assurance activities for each requirement;
- More information must be disclosed across international CCRA Schemes to ensure confidence that evaluations have been consistently performed with the same level of competence and diligence regardless of the CC lab conducting the evaluation; and
- Confidence in a product is limited by its complexity and its separation from other products in the same environment. No amount of documentation and no method of evaluation can overcome these inherent limitations.

3. When and how will the changes be implemented?

Answer: Since 1 October 2009, NIAP/CCEVS policy has been to accept products into evaluation against NIAP approved PPs. For technologies where a PP does not exist, NIAP will work with the vendor, the lab and/or the customer to determine the best way to proceed.

4. What is a Technical Community and how can I participate?

Answer: Technical Communities are being created with NIAP sponsorship for the purpose of creating, maintaining and managing Protection Profiles. NIAP/NSA can no longer be the sole contributor to the PP and needs the expertise of the vendor and lab community. This collaborative effort leverages industry's expertise, is international in scope, provides collective ownership and creates a much needed partnership between industry and government. Vendors, labs, academia and customers are all invited to participate as Technical Communities are created. Due to resource needs, Technical Communities will be created based on the need for new Protection Profiles. If you are interested in participating in a particular Technical Community, contact scheme-comments@niap-ccevs.org.

5. Will the current DOD 8500 policy be affected?

Answer: Yes, NIAP/CCEVS is working with the DOD to update current policies to accommodate the changes. DOD 8500 references the old Robustness model and is being revised. NIAP no longer specifies Robustness (Basic or Medium) within Protection Profiles. When the new DOD 8500.2 is released, it will no longer call out Robustness for evaluated products. NIAP is working will all DOD organizations to update their policies and procedures to remove references to Robustness and Evaluated Assurance Level (EAL).

6. How will the changes affect products already in evaluation?

Answer: Products in evaluation may continue to completion in accordance with the posted CCEVS policies in effect at the time of the acceptance into evaluation. If a vendor is currently undergoing an evaluation under old CCEVS policies either against an outdated PP or no PP, they may choose to evaluate against a new NIAP approved PP without penalty or delay.

7. Will I need to have my evaluated product re-evaluated?

Answer: No, all previously evaluated products will remain certified for the stated version of the product. However, NIAP highly encourages vendors to re-evaluate the product against the new NIAP approved PP. Assurance Continuity continues as stated in current CCEVS Publication #6: "CCEVS – Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0" (http://www.niap-ccevs.org/policy/ccevs/scheme-pub-6.pdf); however the policy is currently being reviewed and may be updated in the future.

8. Once the changes are implemented, if the product has minor changes, may I still update a previously validated product using Assurance Maintenance?

Answer: Yes, CCEVS Publication #6: "CCEVS – Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0" (http://www.niap-ccevs.org/policy/ccevs/scheme-pub-6.pdf) is still in existence and allows for minor changes without re-evaluation. However, if ***major*** changes have been made to the product and a NIAP approved Protection Profile exists, the product must be evaluated against the new PP.

9. When will the NIAP approved Protection Profiles be generated to reflect the NIAP changes?

Answer: NIAP approved Protection Profiles are being written as quickly as resources allow. As of March 2012 the following NIAP approved Protection Profiles are posted to the NIAP/CCEVS web page (http://www.niap-ccevs.org/evolution/pps):

Network Device
USB Flash Drive
Full Disk Encryption
Wireless LAN Access System
Wireless LAN Client
NDPP Extended Package (EP) Stateful Traffic Filter Firewall
IPsec Virtual Private Network (VPN) Clients
Enterprise Security Management – Access Control

10. Will the Common Criteria Recognition Arrangement (CCRA) be affected?

Answer: NIAP/CCEVS is working closely with the CC community to ensure the proposed changes are accepted under the CCRA.

11. Is there still a need for higher assurance products and if so how will they be evaluated?

Answer: Yes, there will always be a need for high assurance products and those products will be evaluated using NSA-approved processes. High assurance products now fall outside the scope of NIAP/CCEVS. If you are a Command/Service/Agency and need further information on the high assurance product evaluation and certification process, please contact your respective NSA Client Advocate using your organization's internal channels. If you are a vendor/developer in need of additional information on the high assurance product evaluation and certification process and have a valid Command/Service/Agency sponsor, please contact the IA Business Affairs Office (BAO) at http://www.nsa.gov/ia/business_research/ia_bao/index.shtml.

12. Will the evaluation Validation Oversight Review (VOR) process remain the same?

Answer: Yes and No. For products starting evaluation under previous CCEVS policies as stated in Question #5 above, the current VOR process remains until the evaluation is complete. For products starting evaluation against a new NIAP approved PP, the VOR process will be replaced with a much less intrusive process. Because the new PPs include more objective assurance activities, there is less subjectivity in evaluator activities and less need for validator oversight throughout the process. The new oversight process is currently under development and will take into account this increased objectivity.

13. Will NIAP accept Protection Profiles developed by other Schemes and Vendor Consortia?

Answer: Yes, NIAP will consider acceptance of any Protection Profile developed by a Technical Community or consortia that has the necessary content to achieve consistent and repeatable results.

14. If a NIAP approved PP does not exist for a technology, will the NSTISSP #11 requirement for evaluation be waived?

Answer: No, NIAP does not have the authority to waive NSTISSP #11 requirements. When a NIAP approved PP does not exist for a technology, NIAP will work with the vendor, lab and/or customer to determine the best way to proceed.

15. Will NSTISSP #11 be updated to accommodate the NIAP changes?

Answer: Yes, NSTISSP #11 was last updated in June 2003 and given the changes in the evaluation and use of COTS and GOTS products, the policy needs to be updated to represent the new NIAP evaluation requirements. CNSSP #11 establishes processes and procedures for the evaluation of COTS and GOTS IA or IA-enabled IT products to be used on National Security Systems. Updates to the policy address the requirements for all COTS to be evaluated and validated as specified by NIAP in accordance with NSA approved evaluation and validation processes. Specific updates included in CNSSP #11 are as follows:

•NSTISSP #11 mandated COTS be evaluated under the Common Criteria or NIAP or FIPS.

•CNSSP #11 mandates:

–COTS be evaluated as specified by NIAP according to NSA approved processes;

–NIAP approved Protection Profiles define the requirements for evaluating COTS, are developed for key technology areas, and will be developed and vetted openly in a public process that includes industry, laboratories, academia and consortia. Protection Profiles will be mapped to NIST Special Publication 800-53 security controls as appropriate (avoid duplicate processes and undue burden on end users; and

–Evaluated COTS products will be listed on NIAP Product Compliant List (which will be populated over time and replaces the current Validated Product list – VPL).

16. If an evaluation starts after 1 October 2009 in another scheme and does not conform to a NIAP approved PP, will it be recognized by NIAP?

Answer: Yes. Certifications by other CCRA schemes remain valid in accordance with that countries' scheme and will be listed on the CC Portal. NIAP is working with members of the CCRA to ensure mutual recognition of NIAP approved Protection Profiles.

17. Can a vendor increase the EAL of the product being evaluated to something greater than specified in the Protection Profile?

Answer: No. Products being evaluated against a NIAP approved PP must be in exact compliance with the PP. No additional testing or evaluation activities will be accepted. If a PP does not exist for a technology, NIAP will work with the vendor, lab and/or customer to determine the best way to proceed.

18. How will the NIAP changes affect the Federal Information Processing Standard (FIPS) 140-2 Level 4 requirements, which state that if an operating system is used it must be EAL4?

Answer: NIAP is working closely with government agencies including NIST to ensure all references to EALs and Robustness are removed from applicable documentation. The majority of this task is complete; however, occasionally an instance will arise where EAL or Robustness is mentioned, usually in regards to product acquisition. In the rare cases where this does happen, we ask that you inform us of this instance and we will work to have the language removed and/or modified.

19. How will a product be listed on the NIAP Product Compliant List (PCL) and the CC Portal Certified Products list?

Answer: For products evaluated by any CC scheme against a NIAP approved Protection Profile, the NIAP PCL will indicate “PP Compliant”; no EAL will be indicated. NIAP is working with the CCRA to also use “PP Compliant” on the CC Portal.

20. **How should I write my Request for Proposal (RFP) when I used to state an EAL requirement?**

    Answer: NIAP will only accept products in for evaluation against a NIAP approved Protection Profile. These PPs will not include an EAL. Therefore, in RFPs, a simple statement of: “… certified in accordance with a NIAP approved Protection Profile” is recommended.