National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

NIAP Policy Letter #30

1 March 2024

SUBJECT: Use of SBOMs in NIAP Common Criteria Evaluations

REFERENCES: National Security Memorandum 8

Committee on National Security Systems Policy (CNSSP) No. 11

M-23-16 Update to Memorandum M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Process

Executive Order 14028 Improving the Nation's Cybersecurity

PURPOSE: This policy defines the requirements for incorporating Software Bill of Materials (SBOMs) into the NIAP Common Criteria Certification Process.

BACKGROUND: Pursuant to CNSSP No.11, NSA's participation in NIAP is to approve evaluation processes for all Commercial off-the-shelf information assurance IT products used on or to protect national security systems. In an effort to increase the sharing of information about cyber threats and improve supply chain security, recent guidance supports the use of SBOMs in federal government procurements.

POLICY: All evaluations and Assurance Maintenance activities submitted to NIAP for evaluation claiming conformance against the Application Software Protection Profile (AppSW PP) or the Application Software Collaborative Protection Profile (AppSW cPP) will be required to include an SBOM. This includes other nation's requests for posting on the NIAP PCL. SBOMs must be submitted as a component of the Check-In and Check-Out package. SBOM documents may be submitted as vendor proprietary. NIAP will perform a review and provide feedback during a mandatory sync session to ensure the SBOM meets requirements and can be incorporated into the vulnerability process. The final SBOM must be approved as part of the evaluation process prior to the product being posted to the NIAP PCL.

Each SBOM must contain the following minimum elements as adapted from the National Telecommunications and Information Administration (NTIA):

SBOM Header Elements:

1. SBOM Author
2. SBOM timestamp
3. SBOM Hash

Component Elements:

4. Component Name
5. Component Version
6. Unique Identifier

7. Component Supplier
8. Dependency Relationship
9. Component Hash
10. Component Data Type

SBOMs will only be accepted in the following formats:

- CycloneDX (v1.4 or above)
- SPDX (v2.3 or above)

EFFECT: This policy provides authoritative guidance on how NIAP will incorporate recent supply chain legislation and policies. This policy only applies to AppSW PP and AppSW cPP but will later be updated to apply to other protection profiles.

EFFECTIVE DATE: All applicable evaluations submitted to NIAP starting March 1, 2024 must conform to this policy. All applicable assurance maintenance activities starting September 1, 2024 must conform to this policy.

Original Signed By

JONATHAN C. ROLF
Director, NIAP

9800 Savage Road, STE 6940, Ft. Meade, MD 20755-6940
Phone: (410) 854-4458 Fax: (410) 854-6615
E-mail: niap@niap-ccevs.org
http://www.niap ccevs.org/