Verslag reacties consultatie SBOM verplichten

Aan:	Forum Standaardisatie
Van:	Bureau Forum Standaardisatie
Datum:	09-11-2026
Versie:	1.0
Bijlage:	1

1.Inleiding

Dit verslag bevat de openbare reacties uit de openbare consultatie SBOM verplichten van het Forum Standaardisatie van 28 juli 2026 tot en met 8 september 2026 op internetconsultatie.nl.

De consultatie is onderdeel van de toetsing van het Forum Standaardisatie of de standaarden CycloneDX versie 1.7 en Software Package Data Exchange (SPDX) versie 2.2 onder de registratie SBOM geschikt zijn om te verplichten aan de overheid (‘Pas toe of leg uit’).

In deze openbare consultatie kon men reageren op het advies van de experts die waren betrokken bij het expertonderzoek voor deze toetsing. Dit expertadvies maakte deel uit van de openbare consultatie.

In de openbare consultatie zijn twee reacties ontvangen. In het volgende hoofdstuk is het antwoord van de respondent een-op-een en ongewijzigd overgenomen van de Pagina reacties van de consultatie.

2.Reacties uit de openbare consultatie

2.1. Reactie van Anoniem

Almere

Datum: 29 juli 2026

De reactie is aangeleverd in de vorm van een brief (zie bijlage).

2.2. Reactie van Anoniem

Amsterdam

Datum: 8 september 2026

2.2.1. Vraag 1

Geef hier indien gewenst uw reactie op het advies van de experts om de standaarden CycloneDX versie 1.7 en SPDX versie 2.2. onder de registratie SBOM (vanaf hier: ‘SBOM’)te verplichten aan de overheid (‘Pas toe of leg uit’) via plaatsing op de 'Pas toe of leg uit'-lijst van Forum Standaardisatie (hoofdstuk 1 van het expertadvies).

“Het lijkt me een goed voorstel om het hebben van SBOM's verplicht te stellen.
Daarbij ook mooi dat er is uitgewerkt welke types SBOM er worden verwacht.
Wat ik alleen mis en wellicht is dat niet per se onderdeel van dit voorstel, is wat de verwachting is m.b.t. de SBOM's nadat deze gegeneerd zijn. Dan zijn er per project een of meerdere SBOM XML of JSON, bestanden, en dan? Helpt dat?
Eigenlijk niet, want ze zijn alleen nuttig als je ze daarna in een ander systeem wil kunnen laden zodat er een analyse op uitgevoerd kan worden.
Zonder dat laatste verplicht je organisaties alleen om die bestanden beschikbaar te hebben, als daar vervolgens niets mee hoeft te gebeuren, dan is het wellicht niet zo zinnig?
Is het bijvoorbeeld voldoende om deze intern op een netwerkschijf of iets dergelijks te hebben staan (met welk doel?), of wil men dat ze ook door anderen ingezien kunnen worden of in een centrale database geladen kunnen worden? Dan zou het verhaal er best anders uit komen te zien denk ik.
Persoonlijk zou mijn feedback dan ook zijn: In plaats van sectie 6 van het expert advies document als adviezen te beschouwen, zouden die wat mij betreft als preconditie moeten worden ingezet om deze standaard door te voeren.
Een ander stukje wat ik mis, is dat er niet wordt gesproken over historie. Een SBOM is een momentopname, wellicht zou het ook fijn zijn om daar een bewaartermijn aan te koppelen. Mocht er dan bijvoorbeeld worden ontdekt dat er 5 maanden geleden een incident is geweest, dan zou men als de bewaartermijn dat toestaat kunnen achterhalen of er ook gebruik gemaakt werd van (externe) code welke een vulnerability bevatte.”

2.2.2. Vraag 2

Geef hier indien gewenst uw reactie op het opgestelde functioneel toepassingsgebied (hoofdstuk 1 van het expertadvies), met name over dat het daarmee aan de inkopende organisatie is om te bepalen welke standaard het beste aansluit bij de specifieke toepassing en situatie (zie ook hoofdstuk 2, paragraaf 1, vraag 5.1.2.1 en 5.1.3.1).

[geen reactie]

2.2.3. Vraag 3

Geef hier indien gewenst uw reactie op het advies van experts om het profiel van het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI) te gebruiken als invulling van een functioneel doel en om duidelijkheid te bieden over de wijze waarop een SBOM wordt ingevuld. (hoofdstuk 1 van het expertadvies).

[geen reactie]

2.2.4. Vraag 4

Geef hier indien gewenst uw reactie op het geformuleerde nut en de geformuleerde mogelijkheden van het gebruik van SBOM voor en door de overheid (hoofdstuk 2, paragraaf 2 van het expertadvies).

[geen reactie]

2.2.5. Vraag 5

Geef hier indien gewenst uw reactie op het doorlopen proces van het expertadvies (hoofdstuk 3 van het expertadvies).

[geen reactie]

2.2.6. Vraag 6

Geef hier indien gewenst uw reactie op de samenstelling van de expertgroep (hoofdstuk 4 van het expertadvies).

[geen reactie]

2.2.7. Vraag 7

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium “Toegevoegde waarde” (hoofdstuk 5, paragraaf 1 van het expertadvies).

[geen reactie]

2.2.8. Vraag 8

Geef hier indien gewenst uw reactie op de vraag of het organisatorisch werkingsgebied goed is gedefinieerd (hoofdstuk 5, vraag 5.1.2.2).

[geen reactie]

2.2.9. Vraag 9

Geef hier indien gewenst uw reactie op de vraag of SBOM meerwaarde heeft boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied (hoofdstuk 5, vraag 5.1.3.2).

[geen reactie]

2.2.10. Vraag 10

Geef hier indien gewenst uw reactie op de vraag of de kosten voor implementatie van SBOM acceptabel zijn en of deze kosten bekend en inzichtelijk zijn (hoofdstuk 5, vraag 5.1.4.1).

[geen reactie]

2.2.11. Vraag 11

Geef hier indien gewenst uw reactie op de vraag of er andere concrete praktijkvoorbeelden (business cases) bekend zijn waar SBOM wordt toegepast (hoofdstuk 5, vraag 5.1.4.2).

[geen reactie]

2.2.12. Vraag 12

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium “Open standaardisatieproces” (hoofdstuk 5, paragraaf 2 van het expertadvies).

[geen reactie]

2.2.13. Vraag 13

Wat is uw mening over het standpunt van experts dat NCSC een geschikte kandidaat is om de rol van Erkend Nederlands intermediair op zich te nemen, dat wil zeggen om de adoptie van SBOM in Nederland actief te stimuleren, betrokken te zijn bij de ontwikkeling rond SBOM en zich inzet op informatiespreiding en kennisuitwisseling (hoofdstuk 5, paragraaf 2.1 van het expertadvies)?

[geen reactie]

2.2.14. Vraag 14

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium “Draagvlak” (hoofdstuk 5, paragraaf 3 van het expertadvies).

[geen reactie]

2.2.15. Vraag 15

Staan volgens u de belangrijkste stakeholders vanuit de overheid voor deze standaarden achter de adoptie van de standaarden (vraag 5.3.3.1 van het expertadvies)?

[geen reactie]

2.2.16. Vraag 16

Staan volgens u de overheidsorganisaties die worden geraakt door een verplichting (‘Pas toe of leg uit’) van de standaarden achter het gebruik van de standaarden (vraag 5.3.3.2 van het expertadvies)?

[geen reactie]

2.2.17. Vraag 17

Worden volgens u de aangemelde versies van de standaarden binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt (vraag 5.3.3.3 van het expertadvies)?

[geen reactie]

2.2.18. Vraag 18

Zijn er volgens u voldoende positieve signalen over toekomstige gebruik van de standaarden door (semi-)overheidsorganisaties, het bedrijfsleven en burgers (vraag 5.3.3.6 van het expertadvies)?

[geen reactie]

2.2.19. Vraag 19

Geef hier indien gewenst uw reactie op de resultaten van de toetsing op hoofdlijnen van hoofdcriterium “Opname op de lijst bevordert adoptie” (hoofdstuk 5, paragraaf 4 van het expertadvies).

[geen reactie]

2.2.20. Vraag 20

Geef hier indien gewenst uw reactie op de aanvullende adoptieadviezen bij verplichting van SBOM door plaatsing op de ‘Pas toe of leg uit’-lijst (hoofdstuk 6 van het expertadvies).

[geen reactie]

2.2.21. Vraag 21

Geef hier indien gewenst uw aanvullend commentaar aan het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) in verband met de inhoud van dit expertadvies en/of het gevolgde proces.

[geen reactie]

Bijlage 1

Ik heb slechts 1 punt van feedback:

Waarom denkt het Ministerie van Volksgezondheid, Welzijn en Sport zich op het gebied van IT standaardisatie te moeten begeven?

Of de aard van het geschetste probleem een legitimatie is voor nieuwe wetgeving is al de vraag, maar ALS er al nieuwe wetgeving moet komen dan is het iets voor ALLE onderdelen van de overheid.

Mijn verzoek is dan ook heel eenvoudig:

STOP met het continu maken van nieuwe wetten, ga eerst eens echt goed nadenken of dit wel zinvol is. Deze consultatie, de nazorg en het voortraject worden allemaal betaald uit gemeenschapsgeld en het geeft geen pas daar op deze ondeskundige wijze mee om te gaan!