Ref. Nr.	Onderwerp	Vraag	Antwoord	
407	Onduidelijkheid vraag 137, 362, 377, 387 en 404 – penetratietesten, verantwoordelijkheid en kosten	Naar aanleiding van de tweede Nota van Inlichtingen hebben wij een verzoek om verduidelijking. De antwoorden over penetratietesten zijn op een aantal punten niet met elkaar in overeenstemming. Omdat dit direct van invloed is op de calculatie, leggen wij dit graag aan u voor. - Volgens het antwoord op vraag 377 zijn de antwoorden op vraag 198 en 256 leidend. Daarmee vallen zowel de periodieke penetratietesten (SEC.12) als de penetratietest vóór inproductiename (SEC.13) binnen de vaste maandvergoeding. - Volgens de antwoorden op vraag 387 en 404 verzorgt Opdrachtgever (Nuffic) de penetratietest vóór inproductiename en valt deze buiten de prijzen in het Prijzenblad. Na inproductiename voert Opdrachtnemer eenmaal per jaar een penetratietest uit. - Volgens het antwoord op vraag 362 vallen onder de SLA technisch beheer, preventief onderhoud, support, incidentafhandeling, minor updates en securitypatches; alle andere werkzaamheden worden later op basis van behoefte bepaald. Penetratietesten worden hierbij niet genoemd. - Volgens het antwoord op vraag 137 bepaalt Opdrachtnemer zelf of de jaarlijkse beveiligingscontrole plaatsvindt door middel van een audit, geautomatiseerde kwetsbaarheidsanalyses of een externe penetratietest. Om alle inschrijvers op dezelfde grondslag te laten calculeren, verzoeken wij u aan te geven: a) of de penetratietest vóór inproductiename (SEC.13) door Opdrachtgever (Nuffic) wordt verzorgd en bekostigd, en het antwoord op vraag 377 op dit punt daarmee vervalt; b) of Opdrachtnemer na inproductiename eenmaal per jaar een externe penetratietest moet uitvoeren, of conform het antwoord op vraag 137 ook kan volstaan met een audit of geautomatiseerde kwetsbaarheidsanalyses; c) onder welke prijsregel in het Prijzenblad de kosten van deze jaarlijkse controle moeten worden opgenomen: de jaarprijs SLA, de jaarprijs Hosting en technisch beheer, of geen van beide; Wij realiseren ons dat de vragentermijn is verstreken. Omdat het hier gaat om onderling tegenstrijdige antwoorden in de Nota van Inlichtingen zelf, die direct van invloed zijn op een gelijke calculatiegrondslag voor alle inschrijvers, verzoeken wij u deze verduidelijking toch te geven.	a: de pentest voor inproductiename wordt door Opdrachtgever verzorgd en bekostigd en hoeft derhalve niet opgenomen te worden in het prijzenblad. b: Het antwoord op vraag 137 volstaat c: Deze kosten vallen onder de post "SLA"	
408	Technische informatie (Nvl 2, ref. 405): beveiligingsrapport en security-overzichten Q3 en oktober 2026; Bijlage 5 SEC.12 en SEC.13; Nvl 2 ref. 137, 377 en 387. Periodieke penetratietest na inproductiename	Bij Nvl 2 heeft u op ons verzoek (ref. 405) het beveiligingsrapport nagestuurd, in de vorm van de security-overzichten van Q3 en oktober 2026. Daarin staat hoe de huidige leverancier updates verwerkt, maar niet of er een periodieke penetratietest is uitgevoerd en wat daarvan de uitkomst was. Over de periodieke pentest na inproductiename geven de antwoorden in Nvl 2 bovendien geen eenduidig beeld: Volgens ref. 387 voert de opdrachtnemer de pentest eenmaal per jaar uit. Volgens ref. 377 valt die test binnen de vaste maandvergoeding. Volgens ref. 137 en 54 bepaalt de opdrachtnemer zelf hoe hij de periodieke controle uitvoert: met audits, geautomatiseerde kwetsbaarheidsanalyses of een externe pentest. Wij verzoeken u aan te geven: a) of de huidige leverancier periodieke pentests op het multisiteplatform en StudyinNL.org heeft uitgevoerd, en of u de laatste rapportage, of een samenvatting van de openstaande bevindingen, met alle inschrijvers wilt delen. Bevindingen uit die rapportage zijn bestaande gebreken die volgens ref. 262 en 328 onder de nulmeting vallen, en ze bepalen mee de omvang van de transitie; b) welk antwoord leidend is: is een jaarlijkse externe pentest verplicht (ref. 387), of mag de opdrachtnemer de periodieke controle uit SEC.12 ook invullen met geautomatiseerde kwetsbaarheidsanalyses en audits (ref. 137)? Wij stellen voor dat Nuffic de jaarlijkse pentest, net als de pentest vóór inproductiename (SEC.13, ref. 85 en 404), zelf laat uitvoeren door een onafhankelijke partij en daarvan de kosten draagt. De opdrachtnemer verleent medewerking en herstelt de bevindingen binnen de termijnen van SEC.12 en ref. 386, binnen de vaste maandvergoeding. Zo blijft de toetsing onafhankelijk van de partij die het platform bouwt en beheert, worden alle inschrijvers op dezelfde basis vergeleken, en blijven de resultaten over de jaren vergelijkbaar. Gaat u met dit voorstel akkoord? Indien u niet akkoord bent en een jaarlijkse externe pentest door opdrachtnemer verplicht is: wat zijn de verwachte scope (aantal websites, acceptatie- en/of productieomgeving, de Studiefinder-API en koppelingen), het type test (black-, grey- of whitebox, geautomatiseerd of handmatig), de eisen aan de onafhankelijkheid en kwalificatie van de testende partij, en de wijze en het moment van rapportage aan Nuffic? Kan die scope over de looptijd meegroeien met het aantal websites in het multisiteplatform, en hoe wordt de prijs dan aangepast?	a) Er zijn op dit moment geen recente pentesten uitgevoerd b) Het antwoord op vraag 137 is leidend. De pentest vóór inproductiename wordt door Opdrachtgever verzorgd en bekostigt, de jaarlijkse pentest (of audit/ geautomatiseerde kwetsbaarheidsanalyse) dient door Opdrachtnemer verzorgt en bekostigt te worden vanuit de jaarlijkse SLA kosten	
409		Uit de aanbestedingsstukken volgt het volgende: - Op grond van §4.2 ("Inschrijven met gegevens van Derden") kan een inschrijver zich beroepen op de technische bekwaamheid van andere rechtspersonen. Een derde op wiens relevante beroepservaring een beroep wordt gedaan, verricht de betreffende diensten zelf. - Volgens het antwoord op Q17 (Nvl 1) geldt de beperking "uitsluitend voor Hosting" in §4.2 alleen voor onderaanneming, en niet voor de wettelijke mogelijkheid om voor geschiktheidseisen een beroep te doen op een derde. - In het antwoord op Q406 (Nvl 2) bevestigt u dat een inschrijver de referenties van een externe partij mag gebruiken, mits deze partij de bijbehorende werkzaamheden daadwerkelijk uitvoert (artikel 2.94 lid 2 Aanbestedingswet 2012). Daar staat het volgende tegenover: - Volgens de antwoorden op Q58 en Q72 (Nvl 1) mag een inschrijver voor onder meer UX-design geen onderaannemers buiten de eigen groep inschakelen. - In het antwoord op Q364 (Nvl 2) bepaalt u dat visueel ontwerp door de groepsmaatschappij mag worden gedaan. Q364 en Q406 staan in dezelfde Nota van Inlichtingen. De rangorderegel uit §2.2 (de meest recente Nota van Inlichtingen prevaleert) biedt hier daarom geen uitsluitsel. Gevolg: een inschrijver die zich voor kerncompetentie 4 ("Ervaring met UX-design, vormgeven en realiseren van WCAG-compliant websites en webfunctionaliteiten") beroept op een gespecialiseerd ontwerpbureau, moet dat bureau op grond van §4.2 en Q406 de ontwerpwerkzaamheden laten uitvoeren. Op grond van Q364 lijkt dat juist niet te mogen. Voor inschrijvers is daardoor niet vast te stellen of een dergelijke inschrijving geldig is. 2. TEGENSTRIJDIGHEID: BEROEP OP EEN DERDE VOOR DE FTE-EIS §5.2.2 stelt onder "Eisen aan studie en beroepsdiploma's" als geschiktheidseis minimaal 2 fte op mbo-niveau en minimaal 6 fte op hbo-niveau (hierna: de fte-eis). In het antwoord op Q384 (Nvl 2) bevestigt u dat dit neerkomt op minimaal 8 relevante fte, waarvan minimaal 6 op hbo/wo-niveau. Volgens het antwoord op Q231 (Nvl 1) tellen daarbij alleen functies mee van medewerkers die in dienst zijn van de inschrijver.	1: de beantwoording op vraag 364 is leidend. Het doel is om een full-service bureau te contracteren welke alle dienstverlening (m.u.v. hosting) binnen hun organisatie (of aan hen gelieerde ondernemingen) over moet beschikken. 2: Zie ook vorige, indien gebruik wordt gemaakt voor aan Opdrachtnemer gelieerde ondernemingen is het toegestaan om hiermee aan de FTE eis te voldoen	
410	Nieuwe wilweg.nl (herhaling vraag 2 uit ons bericht van 10 november)	Volgens het architectuurdiagram is een nieuwe wilweg.nl op het Nuffic-profiel in ontwikkeling. Deze vraag is in Nota van Inlichtingen 2 niet beantwoord. Wat is de verwachte livegang? Als de nieuwe site bij de start van de overeenkomst nog niet live is: valt dan de huidige productieversie onder de as-is transitie, en vallen de afronding en livegang van de nieuwe site buiten de fixed fee voor transitie?	de nieuwe Wilweg website zal voor de transitie live zijn	
411	Vervolgvragen technische informatie	Volgens het architectuurdiagram draait de Studiefinder-API op Laravel Lumen 8. Daarvoor verschijnen geen updates meer. Kunt u bevestigen dat een upgrade of vervanging van deze API buiten de fixed fee voor transitie valt en na de nulmeting als afzonderlijke opdracht wordt overeengekomen?	De meest actuele informatie betreft de API koppeling staat op https://api.hovi.nl/api-opzet/. Mocht deze nog moeten worden vervangen, dan wordt dit niet als onderdeel van de transitie beschouwd en valt het buiten de fixed fee.	
412	Vervolgvragen technische informatie	Het architectuurdiagram noemt een Web Application Firewall voor de Beursopener. Bij welke partij draait deze WAF, en zijn er andere WAF-, CDN- of anti-botdiensten die de opdrachtnemer bij de transitie moet overnemen?	De Web Application Firewall op de beursopener van WilWeg is Anubis. Dit is open-sourcesoftware die wordt door de huidige leverancier beheerd. Er is hiervoor geen externe partij ingeschakeld.	
413	Vervolgvragen technische informatie	Volgens het architectuurdiagram is de Quickscan een gedeelde module in het Nuffic-profiel. Kunt u bevestigen dat de Quickscan op quickscan.nuffic.nl daarmee binnen de as-is transitie valt, en niet vóór de start van de overeenkomst wordt uiteefaseerd?	de oude (fosstaande) quickscan zal worden uitgefaseerd, de nieuwe versie is onderdeel van het multisiteplatform en is daarmee onderdeel van de as-is transitie	