Ministerie van Infrastructuur
en Waterstaat

Bijlage 10.
Samenvatting Marktconsultatie

Onderwerp:	Securitydiensten
Departement:	Ministerie van Infrastructuur en Waterstaat
DG / Directie:	Directie Informatie en Exploitatie (IenE)
Contactpersoon:	Ellen Post Uiterweer
Functie:	Projectleider aanbesteding Securitydiensten
E-mail:	ellen.postuiterweer@minienw.nl
Datum:	1 maart 2022
Versie:	1.0

Inhoudsopgave

Inhoudsopgave 2
1. Inleiding 3
1.1. Aanleiding en doel 3
1.2. Scope 4
1.3. Samenstelling van het team 4
2. Verloop van de marktconsultatie 4
3. Verkregen informatie 4
3.1. Deelname aan aanbestedingsprocedure 4
3.2. Indeling percelen 5
3.3. Risico's huidige beschrijving 6
3.4. Opdrachtgeverschap 7
3.5. Perceelindeling 8
3.6. Specialisme/onderscheid 9
3.7. Suggesties 9
4. Conclusie 10

1. Inleiding

Op 19 oktober 2021 heeft IenW marktpartijen uitgenodigd om deel te nemen aan een marktconsultatie door middel van publicatie van het marktconsultatiedocument "raamovereenkomst Security diensten" op TenderNed.
Doel van de marktconsultatie is om zoveel mogelijk marktpartijen te bereiken, te interesseren en te stimuleren tot meedenken om zo:

- inzicht te verkrijgen in de reële haalbaarheid van het project en in de randvoorwaarden waaronder het project kan worden uitgevoerd;
- input te vergaren voor de aanbestedingsstrategie en de aanbestedingsstukken (nieuwe ideeën opdoen, bestaande ideeën toetsen);
- de markt in een vroeg stadium bij het project te betrekken om de aanbestedingsstukken zo goed mogelijk te kunnen afstemmen op de marktsituatie en de wensen vanuit de markt;
- of de opdracht haalbaar en de gestelde randvoorwaarden realistisch zijn;
- of private partijen interesse en mogelijkheden hebben om de opdracht uit te voeren of te realiseren;
- of de ideeën van IenW passen bij de toekomstige marktontwikkelingen, actieve producten en actieve partijen;
- of de gestelde behoefte zal leiden tot een optimale oplossing voor de eigen organisatie;
- in welke mate er functioneel of technisch gespecificeerd moet worden en welke normen eventueel relevant zijn;
- of er voldoende capaciteit in de markt is;
- of de markt een oplossing heeft voor een functioneel gestelde vraag;
- of er innovatieve oplossingen zijn voor een probleem;
- welke mogelijkheden marktpartijen zien om met minder beschikbaar budget toch aan minimale eisen te kunnen voldoen;
- of er alternatieve oplossingsrichtingen zijn;
- wat de mate van gekwalificeerde opdrachtnemers/leveranciers is;
- of de markt kan voldoen aan de gestelde eisen.

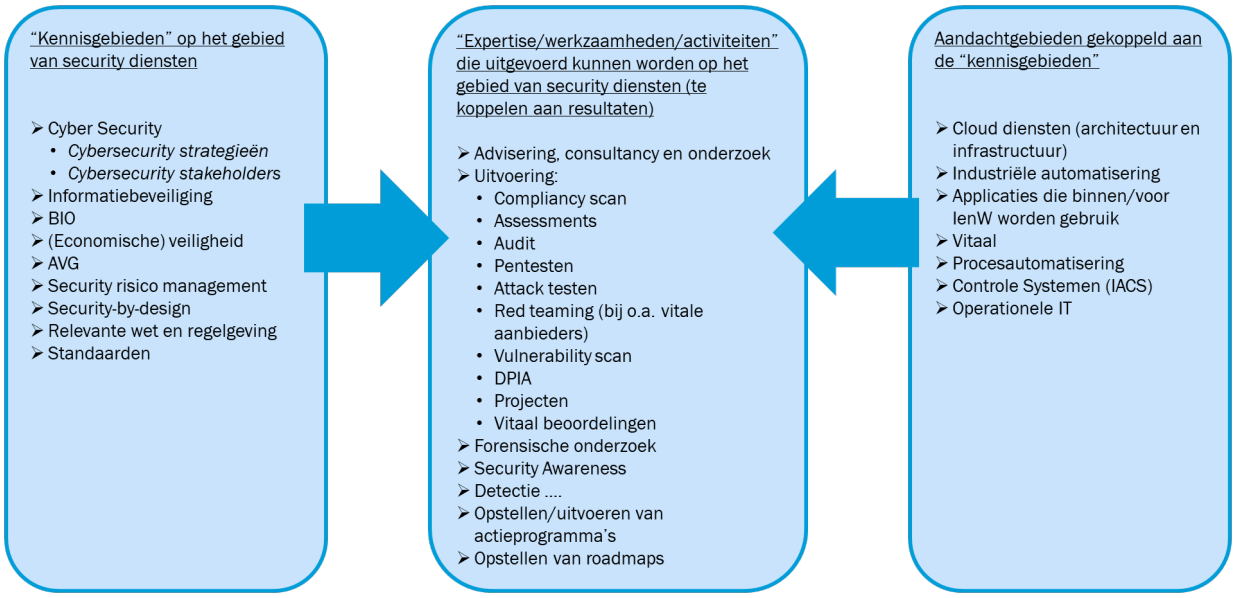
1.1. Aanleiding en doel

Informatiebeveiliging (IB) en Cyber Security (CS) vormen een essentieel en onlosmakelijk geheel van de IenW-processen. Daarnaast groeit het aantal dreigingen in aantal en in ernst. Dit betekent dat we continu adequaat en snel moeten kunnen anticiperen om risico's te mitigeren. De huidige ervaringen leren ons dat het afnemen van noodzakelijk specialistische diensten zoals forensische onderzoeken, pentesten,
dreigingsonderzoeken, etc. bij gespecialiseerde leveranciers veel tijd kost of wegens krapte nauwelijks aanwezig is. Dit kan leiden tot ernstige beveiligingsrisico's.

Met de aanbesteding van een Mantelovereenkomst op het gebied van Cyber Security en Informatiebeveiliging wordt beoogd met een kortere doorlooptijd kwalitatief betere opdrachten te kunnen verstrekken aan gespecialiseerde partijen in de markt.
Daarnaast geeft deze mantel IenW toegang tot de expertise die het niet binnen de organisatie beschikbaar heeft. Door het aangaan van een langere relatie met een aantal vaste partijen is de verwachting dat de uitvoering van een opdracht sneller en kwalitatief hoger zal zijn en dat er beter ingespeeld kan worden op de behoefte.

1.2. Scope

De scope (lijsten zijn niet limitatief, maar zijn richtinggevend)



1.3. Samenstelling van het team

Het team dat deelgenomen heeft aan de marktconsultatie bestaat uit Els de Valk, Marcel de Graaf, Hans Waasdorp, Germain van der Velden, Henk van Halteren, Jules Vetter, Miena Boedhoe en Mellanie van den Berg.

2. Verloop van de marktconsultatie

Vooraf was voorzien dat de marktconsultatie uit twee delen zou bestaan, te weten een schriftelijke vragenronde met aansluitend toelichtende gesprekken. Echter vooralsnog is ervoor gekozen om uit te gaan van de schriftelijk aangeleverde informatie en de gesprekken, mede door de situatie rondom COVID, vooralsnog niet plaats te laten vinden, tenzij gaandeweg blijkt dat een nadere toelichting toch gewenst is..

Naar aanleiding van de marktconsultatie is informatie ontvangen van de 16 marktpartijen.

3. Verkregen informatie

Onderstaand een samenvatting van de beantwoording op de gestelde vragen.

3.1. Deelname aan aanbestedingsprocedure

Wat zouden voor u redenen kunnen zijn om wel of niet deel te nemen aan de aanbestedingsprocedure?

Redenen om deel te nemen:

- Deelname past in de bedrijfsstrategie.
- Goed inzicht in de beoogde afname op korte en middellange termijn
- Gezonde balans in prijs en kwaliteit waarbij kwaliteit leidend zou moeten zijn
- Het aantal te contracteren partijen dient in balans te zijn met de opdracht
- ARBIT is niet geschikt voor alle onderdelen van de genoemde scope, aanpassing van de voorwaarden moet mogelijk zijn voor die onderdelen.
- Aansprakelijkheid proportioneel in verhouding tot opdrachtsom

- De mogelijkheid om het portfolio/communicatie ook in het Engels te kunnen leveren
- De mogelijkheid een beroep te kunnen doen op expertise binnen de eigen organisatie in landen buiten de EER
- Werkgebied uitbreiden van commerciële sector naar publieke sector
- Een realistisch gevraagde inspanning in relatie op kans op selectie

Redenen om niet deel te nemen:
- Ongunstige voorwaarden of boeteclausules die niet afgestemd zijn op omvang van de opdracht
- Een te grotere capaciteitswens dan beschikbaarheid binnen de organisatie
- Indien contractwaarde niet in balans is met de gestelde eisen/wensen, selectie en gunningcriteria.
- Aanbiedingsplicht, gezien schaarste op de markt
- Een zodanige opdeling in percelen waardoor de kwaliteit van de gevraagde diensten in het gedrang zou komen
- In geval van toepassing niet realistische maximum (uur)tarieven
- Een te nauwe of juist een te ruime indeling in percelen
- Indien er geen level play field bestaat, de te denken aan te zware selectie of gunningseisen
- Een voldoende grote omvang en winstkans bij nadere overeenkomsten
- Indien de partij niet aan de gestelde eisen kan doen of teveel afhankelijk zou worden van een consortium of onderaannemers

Overige genoemde aanbevelingen:
- Of en hoe kleinere partijen deel kunnen nemen hangt af van de wijze van indeling in percelen en de gewenste specialisatie binnen de percelen.
- Een partij zou specifiek op haar kennisgebied moeten kunnen inschrijven
- Het one-stop principe zou een beperking in kwaliteit en aanbod vormen

3.2. Indeling percelen

Welke dienstverlening moet u in combinatie aanbieden?
Van de 16 deelnemende partijen aan de marktconsultatie geven 4 partijen aan alle gevraagde dienstverlening te leveren, hoewel dat door één partij in de beantwoording van een volgende vraag weer tegengesproken wordt doordat verzocht wordt audits buiten een perceel te laten, 3 partijen kunnen alles leveren met uitzondering van forensisch onderzoek. Een 6-tal partijen geeft aan de gevraagde diensten deels via partners of in combinatie te kunnen leveren. De overige partijen geven geen duidelijk antwoord.

Hoe kan naar uw mening door aanpassing van de voorgestelde scope van de aanbesteding een betere aanbieding door u worden gedaan?
- De scope zou verbeterd kunnen worden door een verdiepende slag aan te brengen en de onderlinge samenhang uit te werken/toe te lichten
- Onderwerpen als bijv. penetratietesten, vulnerability scanning) lenen zich beter om deze in losse uitvragen op te knippen
- Knip de aanbesteding in drie percelen voor 3 typen organisaties uit de markt:
  - Nationaal overkoepelend beleid voor grotere adviesbureaus en voor het samenstellen, continu actualiseren en bewaken van generieke richtlijnen voor alle subdomeinen binnen het Ministerie
  - Specifiek maken van de overkoepelende en generieke richtlijnen per subdomein, voor kleinere uitvoeringsbedrijven
  - Raamovereenkomsten met 10 partijen per organisatietype
- Geef aanbieders de kans te zelf met mogelijkheden te komen om aanvullende diensten voor te stellen
- Een partij beveelt aan:

  - Door mogelijk benodigde in te zetten hard- en/of software tools en ook 'managed security services' op te nemen in de scope
  - SIEM-services toe te voegen aan de scope
  - Sourcing van preffered security-partners van de deelnemers op te nemen in de scope, zodat reeds ingezette dienstverleningsovereenkomsten voortgezet kunnen worden onder deze ROK. Bijvoorbeeld in de vorm van een zgn 'technisch gespecificeerde uitvraag.
- Geef a.u.b. de context vanuit zowel organisatie als techniek. Een nadere invulling
- Geef aan welke security-frameworks worden toegepast en welke compliancy van toepassing is
- Denk na over toevoeging van een losse meerjarige dienst voor strategisch advies dat gedurende de volle looptijd wordt afgenomen (=trusted partner)
  Dan wel andere partij(en) nodig voor de toetsing hiervan.
- Zorg voor een coherente aanpak; de wijze waarop cybersecurity wordt aangevlogen is van grote invloed op het eindresultaat.
- Een heldere scope beschrijving van de aanbesteding, in termen van:
  - Duur en omvang van de raamovereenkomst;
  - Duidelijkheid over aantal verwachte opdrachten per jaar en per gevraagd onderdeel;
  - Of het de gevraagde diensten als project geleverd worden of als operationele dienst (en met welke Service Levels);
  - Welke governance structuur voorzien wordt;
  - De verkaveling van gevraagde diensten;
  - Verduidelijking welke bestaande leveranciers geraakt worden, zoals Rijks Data Centra en bestaande ICT-beheerpartijen;
  - Specificatie van benodigde certificeringen (zoals CISSP, OSCP, CIPP etc) en vereisten t.a.v. screening van ons personeel (VOG of AIVD-veiligheidsonderzoek);
  - Verwachtingen aan de leveranciers t.a.v. servicemanagement, governance en rapportage;
  - Eisen aan omvang van de leverancier, aansprakelijkheid, vertrouwelijkheid, AVG, etc;
  - Bereidheid of wensen ten aanzien van innovatie binnen de dienstverlening.
- Geef een duidelijke definitie van de gevraagde diensten. Dit het liefst gebaseerd op wat speelt er op dit moment, wat is de aanleiding, waarom deze uitvraag en indeling, wat is de gedachte hierachter, wat zijn de dagelijkse onderzoeksvragen of problemen binnen cybersecurity? Wat is het kernprobleem? Wat willen jullie oplossen/realiseren? Wanneer zijn jullie tevreden."
- Opdeling in percelen voor preventief testen, incident gedreven diensten, awareness en beleidsmatige diensten om zo de beste partijen per onderdeel te kunnen selecteren.
- Maak onderscheid tussen OT (gericht op de operatie van de OT installaties, waaronder industriële- en proces automatisering) en IT (gericht op de interne bedrijfsprocessen en informatie binnen organisaties en bedrijven) omdat voor beide aandachtsgebieden specifieke expertise nodig is.

3.3. Risico's huidige beschrijving

Wat zijn de nadelen en risico's van de huidige beschrijving?

- De huidige beschrijving gaat (nog) niet in op resultaat- versus inspanningsverplichting. Een resultaatverplichting stelt hoge eisen aan beide partijen. In de praktijk blijkt het lastig te zijn om eenduidige requirements af te geven. Daarom advies om de opdracht te splitsen in deze twee vormen.
- Meer diepgang in de beschrijving van de scope is gewenst met risico dat bepaalde onderbelicht blijven, niet geadresseerd worden of dat inschrijvers hun eigen interpretatie erop los kunnen laten.

- De uitvraag lijkt met name gericht te zijn op security-only-bedrijven. Uitvoeringsbedrijven (met specifieke domeinkennis) zouden ook toegang moeten krijgen. De uitvraag kan leiden tot een lock-in van één marktpartij en het ontbreken van checks-and-balances, waardoor veiligheid juist brozer wordt. Een Certifying Agent moet ook beoordeeld kunnen worden door een andere Certifying Agent en moet ook het nationale beleidskader kunnen toetsen.
- De huidige beschrijving maakt het lastig om tot een coherente securityaanpak te komen
- Het overgrote deel van de gevraagde expertisediensten zijn projecten met een spreekwoordelijke kop en staart. Deze maken normaliter deel uit van een overkoepelende MDR-dienst die meeromvattend is. Een dergelijke dienst ontlast organisaties van veel van de werkzaamheden die horen bij het detecteren van en response op security incidenten zodat de eigen security specialisten vrijgemaakt worden voor werkzaamheden die de specialistische kennis van de eigen medewerkers vereist.
- "In de huidige bijlage van de uitvraag wordt gesteld; 'Kennis van deze processen, de impact van verstoringen en het overkoepelende beleid is een onmisbare eigenschap'.
- Door het stellen van deze eis, kunnen potentiële aanbieders mogelijk niet gaan reageren. Aanbieders die wel de gezochte cyber security/informatiebeveiliging kennis hebben, maar niet de proceskennis. Onze gedachte is dat met een goed samenspel, de proceskennis ook vanuit de eigen organisatie kan worden aangedragen.

3.4. Opdrachtgeverschap

Kunt u op basis van ervaring wat zeggen over het gedrag van de ideale opdrachtgever?

- (strategisch) partnerschip: transparantie/ samenwerken/ vertrouwen / gefocust op resultaat en voor langere termijn.
- Een goede governance, duidelijke en afgestemde communicatielijnen en een escalatietrap voor dreigingsadvies
- Oog voor kwaliteit, niet alleen focus op prijs
- Laat de partner het hoe bepalen (binnen een afgekaderde resultaatverplichting); m.a.w. ga niet op de stoel van de opdrachtnemer zitten
- De ideale opdrachtgever heeft zelf ook securitykennis in huis (deskundige opdrachtgever);
- Daadkracht, besluitvaardigheid en knopen doorhakken
- Geeft openheid over roadmaps en behoeften van deelnemers
- Coördineert/ondersteunt methodiek van uitvragen en gunnen door deelnemers
- Kent zowel de opdrachtgevers als de deelnemers en is ambassadeur voor beiden
- Stelt geen onredelijke eisen en staat open voor feedback
- Eerlijk/transparant proces voor minicompetities met voldoende tijd
- Globale planning komt hierin terug, de minicompetitie een te korte planning opnemen.

Welke mindset heeft deze ideale opdrachtgever?

- Partnerschap, samenwerking
- Security bewustzijn binnen alle lagen van de organisatie.
- Opdrachtgever is beweeglijk/adaptief (snelheid van wijziging van het dreigingslandschap vraagt om snel kunnen handelen
- Besluitvaardigheid
- Openstaan voor verandering en innovatiekracht
- Constructief, positief-kritisch en voorwaarts gericht
- Indien nodig dient de securitypartner toegang te krijgen of alle rapporten en informatie uit onderliggende projecten om de klant zo goed mogelijk te kunnen bijstaan
- Openheid en transparantie
- Eerlijk en ethisch, gericht op bevindingen

- Niet bang om kritiek te ontvangen of te geven
- Bereid om oorzaken van gesignaleerde probleem aan te pakken i.p.v. het gevolg
- Oog voor kostenaspect van minicompetities voor relatief kleinere projecten
- Evalueren, ontwikkelen en verbeteren

Wat is in uw ogen goed opdrachtgeverschap en hoe is dat ingeregeld?

- Transparante projectplanning
- Continue dialoog met de marktpartijen
- Duidelijke beschrijving van gevraagde diensten
- Organiseren van dialoogsessies om inschrijvers via vraag en antwoord meer inzicht te verschaffen
- Is op de hoogte van de marktontwikkelingen (bijv. op gebied van personeelsbezetting)
- Per project: contactpersoon/projectsponsor, heldere scope, deliverables, heldere planning en overlegstructuur, commitment op toegezegde medewerking
- Algemeen: regulier overleg over planning toekomstige uitvragen en periodieke evaluaties over de dienstverlening (=contract/leveranciersmanagement)
- Kleinere opdrachten rechtstreeks te gunnen.

3.5. Perceelindeling

Uitgaande van de verwachte scope/onderwerpen van de aanbesteding, adviseert u ons te kiezen voor een perceel indeling?
Zo ja, welke zou dan volgens u het beste werken? Zo nee, waarom niet?

- Het uitvoeren van uitvoeren van DPIA's en forensics vergt specifieke opleiding en/of certificeringen. Stelt daarom voor volgende indeling te maken:
  - Compliancy en vulnerability diensten
  - Forensic diensten
  - Advies en consultancy
- Forensics en in mindere mate pentesting in aparte percelen kunnen. Forensics vraagt hele specifieke expertise die slechts een paar partijen kunnen bieden. Pentesting is bijna een commodity service geworden.
- De grotere partijen adviseren om één perceel toe te passen. Motivatie: integraliteit van de genoemde onderwerpen.
- Managed services in een apart perceel onder te brengen gezien de significant andere contract-, relatie- en dienstvorm.
- Een partij beveelt twee percelen aan:
  1) Beleid: vitaal beoordelingen, roadmaps, actieprogramma's, audits, en red teaming. (3 contractpartijen)
  2) Expertise services: ondersteunende en uitvoerende diensten. (3 contractpartijen)
- Een andere partij beveelt aan om in 3 percelen op te delen met 3 tot 5 partijen per kavel. Motivatie: de scope van de dienstverlening is verschillend van aard. Verkaveling leidt tot deelname kleine specialistische bedrijven. Eén groot perceel zou het level play field verstoren omdat alleen grote bedrijven succesvol kunnen aanbieden.
  Roteren tussen partijen om tot nieuwe inzichten te komen in staat van beveiliging.
  - Kavel A: Strategisch/tactisch advies en consultancy security & Privacy
    Advies en consultancy op gebied van security, privacy (bijv. DPIA'S) en robuustheid ICT-infrastructuur en Applicaties.
  - Kavel B: Technische Security assessments
    Technisch onderzoeken en toetsen van de getroffen securitymaatregelen en advisering over noodzakelijke verbeteringen.

(Compliancy scans/assessments/audits, vulnerability scans/assessments, Pentesten en attack testen, Hardening onderzoeken
    - Kavel C: Incident response (Forensics bij security incidenten en Forensics / intelligence; onderzoeken naar bedreigingen
- De benoemde scope zou werken. Aandachtspunt: bedrijven moeten wel een breed portfolio hebben op cybersecuritygebied: pentesting, red teaming, consultancy, forensische analyse, awareness.
- Gezien de verschillen in knowhow en expertise de volgende percelen te definiëren welke ieder onderverdeeld zijn in de sub percelen consultancy, implementatie, operationeel:
    - Perceel 1: Informatiebeveiliging. Gericht op IT voor kantoorautomatisering (waarbinnen mobiele- en ERP applicaties en Cloud).
    - Perceel 2: OT cyber security. Gericht op Industriële automatisering, Proces automatisering, Controle systemen en Operationele IT.

3.6. Specialisme/onderscheid

Wat is uw specialisme, waarom bent u hier goed in en hoe groot is uw bedrijf?

De bedrijven zijn soms specialistisch, soms breed georiënteerd die veelal Europees of internationaal opereren. Een van de bedrijven heeft zich gespecialiseerd in sourcing van ICT Dienstverlening.

3.7. Suggesties

Heeft u nog andere ideeën, suggesties of opmerkingen of ziet u nog risico's of uitdagingen voor IenW met betrekking tot de voorgenomen aanbesteding?

Gedane suggesties:
- Sluit aan bij de Rijksbrede ROK resultaat verplichte opdrachten
- Selecteer één partij versus voorkom dat je vast komt te zitten aan één contractpartij
- Selecteer enkele full service partijen
- Selecteer alleen op kwaliteit, niet op prijs (prijs alleen in minicompetities)
- Gebrek aan kwaliteit wordt soms gecompenseerd door lage tarieven
- Goede kwaliteit vergt investering in voortdurende opleiding van personeel
- Laat partijen zich kwalificeren op basis van bijv. een proeve van bekwaamheid (pentest of code review) of een goede casus waarin de complexiteit van de opdracht naar voren komt
- Het is aantrekkelijk om in te schrijven op een variant waarbij gewerkt wordt met een roulatieschema waarbij de leveranciers over de periode evenveel opdrachten doen
- Meerdere partijen adviseren een niet-openbare aanbesteding te doen.
- Beperk de nadruk op (uur)tarieven
- Neem ook managed services of privacy services op in de scope
- Om een niveau van kwaliteit te garanderen de noodzaak voor een CCV-certificering verplicht stellen. https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/
- Neem een mechanisme op ter beloning van geboden kwaliteit met bonusregeling (bijv. toeslag op tarieven, grotere kans op gunning van een opdracht)
- Voor bepaalde onderzoeken zijn cliënten minder geneigd om referenties af te geven. Bijvoorbeeld bij forensische onderzoeken of onderzoeken naar de vitale infrastructuur. Deze laatste categorie zijn vaak gerubriceerd.

4. Conclusie

Een 16-tal bedrijven hebben deelgenomen aan de marktverkenning. De meeste bedrijven opereren internationaal. Alle geven zij aan geïnteresseerd te zijn in deelname aan de aanbesteding, mits de omvang van de opdracht inzichtelijk is, het aantal te contracteren partijen in balans is met de opdracht, de voorwaarden proportioneel en passend zijn bij de aard van de opdracht en er een gezonde balans is in prijs en kwaliteit.

De bedrijven hebben een verschillende kijk op de beste onderverdeling in percelen; deze lijkt met name ingegeven te zijn op basis van hun eigen positie in de markt. Naar voren komt dat het one-stop principe een beperking in kwaliteit en aanbod zou kunnen vormen, anderzijds zou het opknippen in percelen leiden tot versnippering, hetgeen een coherente aanpak in de weg zou staan.

Het voorwerp van de aanbesteding bevindt zich in een schaarse markt die volop in ontwikkeling is. Er is meer diepgang in de vraagstelling nodig om goed te kunnen aanbieden. De meeste bedrijven lijken te opteren voor een strategisch partnerschap gefocust op resultaat en voor langere termijn. De bedrijven geven aan behoefte te hebben aan een daadkrachtige, inhoudelijk deskundige opdrachtgever. Daarnaast is er behoefte aan een duidelijke governance en een aanspreekpunt vanuit IenW voor regulier overleg over planning van toekomstige uitvragen en periodieke evaluaties over de dienstverlening.