Nr	Ref	Pag	Vraag	Antwoord
			MARKTCONSULTATIEDOCUMENT	
1	ALGEMEEN Nummering		Medeling	De nummering het marktconsultatiedocument is vanaf 3.1 incorrect doorgenummerd. Dit is in de nieuwe versie aangepast. **Onderstaand wordt in de kolom referentie (ref) de gecorrigeerde nummering en mogelijk daardoor gewijzigde paginanummering aangehouden.**
2	ALGEMEEN Invulformulier		Kunt u ons omwille van efficiëntie en het voorkomen van fouten een bewerkbaar document geven waarin de vragen staan?	In "Documenten" op TenderNed is inmiddels een bewerkbare Word-versie ge-upload van de vragen in het marktconsultatiedocument. Als het uw gemak kan dienen staat het u vrij deze voor uw beantwoording te gebruiken. In het kader van onze verwerking van uw reacties heeft dit Word-document (of vergelijkbaar) ook onze voorkeur.
3	Deelnemers	1	U geeft aan de diverse ministeries en enkele ZBO's mee gaan doen met de aanbesteding. Kunt u dat concretiseren in aantallen en eventuele namen van de betrokken organisaties?	Alle ministeries doen mee met het collectief van de diverse IB-gerelateerde aanbestedingen, maar er is wisselende deelname per ministerie, onderliggend organisatieonderdeel en/of het perceel. Organisatie die ressorteren onder de ministeries en aan geen van de IB-percelen deelnemen zijn: de Belastingdienst, DICTU, AIVD, NEa en enkele raden/colleges van het ministerie van OCW. Daarnaast hebben diverse zelfstandige bestuursorganen met eigen rechtspersoonlijkheid, hoge colleges van Staat, een sui generis organisatie de intentie om deel te nemen: Algemene Rekenkamer, Eerste kamer der Staten-Generaal; Tweede kamer der Staten-Generaal, Raad van State, Hoge Raad der Nederlanden, Nationale ombudsman, CAK, CBR, COA, KvK, Kansspelautoriteit, NZa, Raad voor de Rechtsbijstand, SVB, Stichting Reclassering Nederland, Stichting Slachtofferhulp Nederland. E.e.a. is onder voorbehoud van wijzigingen. Een definitieve en gespecificeerde lijst van deelnemers zal bij de betreffende aanbesteding(en) worden gegeven.

Nr	Ref	Pag	Vraag	Antwoord
4	1.3 Volwassenheid deelnemers	3	In het document wordt een brede verscheidenheid aan diensten uitgevraagd, er wordt echter geen duidelijkheid gegeven over de volwassenheid van de deelnemers en de bereidheid tot verandering. Wat heeft u voor ogen na de uitvoering van de marktconsultatie, het inkopen van losse diensten of ook een transformatie?	Van specifiek volwassenheid op de IB-onderdelen is geen overkoepelend overzicht te geven. Daarvoor is het deelnemersveld te groot en divers. De nadere opdrachten zullen per geval bepalen in hoeverre een losse dienst wordt verzocht, dan wel daarbij ook transformatie.
5	1.3 2021/2025	3	Paragraaf 1.3. Bij de vorige RVICTO-aanbesteding in 2021 waaraan u refereert, was het niet mogelijk om zowel op perceel 1 (alle profielen m.u.v. paragraaf KWIV 4.1) als perceel 2 (Informatiebeveiliging) in te schrijven. Wij lezen nu dat er bij de nieuwe RVICTO-aanbestedingen sprake zal zijn van twee separate aanbestedingen. Is onze aanname juist dat het nu mogelijk zal zijn om op beide aanbestedingen in te schrijven, en dat deze elkaar niet uitsluiten?	U lijkt te verwijzen naar paragraaf 1.4.2 (TN332318) op pagina 10 van het aanbestedingsdocument uit 2021: Een inschrijver kan uitsluitend op één van de genoemde percelen inschrijven. Voor de onderhavige IB-onderwerpen is onderling zulks niet voorzien voor de nieuwe aanbestedingen. Het is wel mogelijk dat bij minicompetities/opdrachten binnen de beoogde raamovereenkomsten opdrachtnemers kunnen worden uitgesloten van deelname als er een onacceptabel risico op belangenverstrengeling ontstaat. Bijvoorbeeld om te voorkomen dat een opdrachtnemer een informatie-beveiligingsonderzoek zou moeten uitvoeren op een systeem dat hij zelf heeft gebouwd. Als u hierover beelden hebt die de aanbestedingsstrategie richting de organisatiedoelen kunnen versterken, dan vernemen wij die graag.
6	1.3	3	In de huidige situatie (TN332318) is deelnemen aan beide raamovereenkomsten door 1 leverancier uitgesloten. U geeft aan dat Perceel 1 binnen RVICTO 26 een separate aanbesteding gaat worden. Betekent dit dat genoemde uitsluiting binnen RVICTO 26 niet van toepassing gaat zijn?	Zie antwoord op vraag 5.
7	1.3	3	In de huidige situatie (TN332318) is deelnemen aan beide raamovereenkomsten door 1 leverancier uitgesloten. U geeft aan dat Perceel 1 binnen RVICTO 26 een separate aanbesteding gaat worden. U overweegt voor Perceel 2 een aantal (4) raamovereenkomsten af te sluiten. Voorziet u dat deelname aan 1 raamovereenkomst mogelijk lijdt	Zie antwoord op vraag 5.

Nr	Ref	Pag	Vraag	Antwoord
			tot uitsluiting van deelname aan een andere overeenkomst? Zo ja, welke?	
8	1.3 ROK	4	U schrijft in 1.3 dat u voor de benoemde typen IB diensten aparte raamovereenkomsten wilt sluiten. Kunt u verduidelijken of u per benoemd type dienstverlening van plan bent een mantel af te sluiten (hier: 4 mantels), of beoogt u één mantel af te sluiten voor deze typen diensten?	Met 'aparte raamovereenkomsten' bedoelen we een raamovereenkomst voor Pentesten, een raamovereenkomst voor Red Teaming en een raamovereenkomst voor SOC-diensten. Per raamovereenkomst beogen we een verschillend aantal contractpartijen. Zie ook de vragen hierover. Voor Overige IB-diensten is nog niet uitgemaakt hoe deze in overeenkomst worden gegoten, daar het een zeer grote verscheidenheid aan type dienstverlening betreft. Als u hierin goede ideeën hebt vernemen we die uiteraard graag.
9	1.3	4	Op pagina 4, onderaan tweede alinea stelt u: "Het idee is om voor deze typen IB-dienstverlening aparte raamovereenkomsten te sluiten. De vragen in deze marktraadpleging zien op deze IB-dienstverlening." Als ik het goed begrijp zijn deze diensten onderdeel van deze RFI en RFP, maar komt er een aparte raamovereenkomst. Klopt dit?	Zie het antwoord op de vorige vraag.
10	1.3.4 Incident response	5	In de huidige indeling van onderwerpen binnen RVICTO26 wordt het thema "resilience" (digitale weerbaarheid) slechts indirect behandeld, bijvoorbeeld via Red Teaming, SOC-diensten en incident response. Kan "resilience" als een zelfstandige werkstroom toegevoegd worden? Hierbij met focus op: - Organisatorische weerbaarheid: hoe snel en effectief organisaties kunnen reageren op verstoringen. -Cyber resilience assessments: maturity scans, stresstests, en simulaties van verstoringen. -Continuïteitsplanning en herstelvermogen: integratie van IR, forensisch onderzoek en business continuity. -Resilience-by-design: advies over architectuur, redundantie en failover-mechanismen.	Dank voor uw suggesties. De door u benoemde onderwerpen zijn inderdaad nog niet expliciet benoemd.

Nr	Ref	Pag	Vraag	Antwoord
			Wij stellen voor om "resilience" als zelfstandige werkstroom of horizontaal thema te positioneren. Dit omvat o.a. organisatorische weerbaarheid, maturity assessments, herstelvermogen en resilience-by-design. Wij missen in het bijzonder het expliciete onderdeel Cyber Recovery: het herstel van systemen en data na een cyberincident. Wij stellen voor dit als herkenbaar onderdeel op te nemen binnen de scope, gezien de toenemende relevantie in het licht van NIS2, CRA en ransomwaredreigingen	
11	1.4	7	De geschatte omvang per onderwerp heeft in bepaalde gevallen een grote range. Wordt deze range ten tijde van de aanbesteding preciezer gemaakt en kunt u aangeven op basis waarvan de huidige ranges zijn bepaald?	De huidige raming zijn de optelling van schattingen van deelnemers. Ze drukken in deze marktraadpleging een orde van grootte uit. In de aanbesteding zullen deze verder worden geconcretiseerd en zal nader verfijning plaatsvinden, zowel qua raming als de zekerheid en het profiel van deelname van deelnemende organisaties.
12	1.6	8	Op pagina 9, bovenste alinea vermeld u: "Deelnemers zijn verantwoordelijk voor het beoordelen of bij een nadere opdracht mogelijk sprake is van een nationaal veiligheidsbelang. Veiligheidsmaatregelen kunnen zich doen gelden in het inkoopproces, als ook in de uitvoering. Dit kan de aanbestedingsstrategie voor de Europese Aanbestedingen voor raamovereenkomsten raken, als ook concrete (nadere) opdrachten. Dit brengt een voorbehoud op de mogelijke indrukken en verwachtingen die met dit document gewekt kunnen worden". Op dit moment zijn wij nog niet ABRO gecertificeerd. Wij zijn wel bereid het proces in te gaan. Is de intentie, met een commitment als we worden toegelaten tot de mini competities voldoende om deel te kunnen nemen aan de RFI en later de RFP? Graag bevestiging.	Er is momenteel nog geen ABRO waarop u kunt worden getoetst. Deze zal naar verwachting in de komende tijd worden vastgesteld (in ieder geval in de contractperiode van RVICTO 2026) en hierna tranche-gewijs worden geïmplementeerd. RVICTO wil zoveel als mogelijk hierop zijn voorbereid. Een toekomstige ABRO-autorisatie op het niveau van een raamovereenkomst mag u zien als een voorwaardelijke autorisatie. Deze kan dan slechts worden verstrekt voor een beperkt aantal beveiligingseisen, waarop het NBIV u kan toetsen. Voor gerubriceerde/gevoelige opdrachten binnen de raamovereenkomst zal telkens een (eigen) autorisatie nodig zijn. Aan welke beveiligingseisen van de ABRO voldaan moet worden, kan per opdracht (w.o. het rubriceringsniveau) verschillen. Deelname aan de minicompetitie is in principe wel mogelijk, maar zonder autorisatie kunt u niet starten met een dergelijke gerubriceerde/gevoelige opdracht. Voor niet-gerubriceerde/gevoelige opdrachten is geen ABRO-autorisatie nodig.

Nr	Ref	Pag	Vraag	Antwoord
			Pentesten	
13	3.1 Raming	13	Is de vermelde financiële omvang (10-50k) en het aantal pentesten (800-2500) per jaar of voor het totaal aantal jaren?	De vermelde financiële omvang is 10-50 miljoen over het totaal van vier jaar.
14	3.1 Raming	13	Kan de aanbestedende dienst aangeven op basis van welke criteria deze inschatting is gemaakt. Gezien ook TIBER-niveautests verwacht worden.	De raming is gebaseerd op opgaven van deelnemers. TIBER-niveautests maken hier geen deel van uit. Die zijn begrepen onder het deel Red Teaming.
15	3.1 Prijs/kwaliteit	13	Kunt u aangeven wat de verhouding is tussen prijs en kwaliteit in de raamovereenkomst? Hanteert u een minimumaantal punten op kwaliteit om deze zo te waarborgen?	Op dit moment is de Prijs/Kwaliteit-verhouding voor de aanbestedingen van de Raamovereenkomsten nog niet bepaald, als ook niet voor de nadere overeenkomsten.
16	3.1 Raming	13	Wat voor soort pentest-oefeningen worden er uitgevoerd, en kunt u een indicatie geven van de omvang (bijvoorbeeld 200 interne BlackBox-tests, 300 externe webapplicaties GrayBox, 10 applicaties)? Als er interne pentests nodig zijn, zijn dan alle locaties in Nederland (of bv ook de antillen)?	Een nadere onderverdeling van pentesten naar b.v. black/grey/whitebox is nu niet te geven. Hetzelfde geldt voor b.v. geteste objecten. De pentesten kunnen uitgevoerd worden vanuit diverse locaties in Nederland en (incidenteel) Caribisch Nederland.
17	3.1 EER	13	Kunt u aangeven voor welk deel van de pentesten u het noodzakelijk acht dat deze volledig vanuit de EER worden uitgevoerd en dat de uitvoerders allemaal gescreend zijn?	Met betrekking tot uitvoering in de EER: in principe alle delen binnen EER en Caribisch Nederland onder werking van de AVG en straks de CBW. Als u daar (structureel/incidenteel) noodzakelijke afwijkingen op ziet, vernemen we die graag en waarom die noodzakelijk zijn. Met betrekking tot veiligheidsonderzoeken/screening van personen: Per aanvraag/opdracht zal aangegeven worden of een veiligheidsonderzoek nodig is en zo ja, op welk niveau. Het is denkbaar dat een groot gedeelte van de in te zetten professionals een veiligheidsonderzoek moet ondergaan en een zogenaamde ‘verklaring van geen bezwaar’ moet kunnen aantonen.

Nr	Ref	Pag	Vraag	Antwoord
18	3.1 Lokatie	13	Kunt u aangeven voor welk deel van de pentesten u het noodzakelijk acht om op locatie van de deelnemer te testen?	Nee, dat kunnen wij nu nog niet aangeven.
19	3.1 Scope	13	In de huidige scope van pentesten binnen RVICTO26 wordt geen expliciete aandacht besteed aan pentesten op operationele technologie (OT), zoals industriële controlesystemen (ICS), SCADA-omgevingen en andere cyberfysieke systemen. Kan deze vorm van pentesten expliciet opgenomen worden in de scope van de pentest-workstream? Want: -OT-omgevingen zijn steeds vaker doelwit van geavanceerde aanvallen (bijv. ransomware, statelijke actoren). -De impact van kwetsbaarheden in OT is vaak direct fysiek en maatschappelijk ontwrichtend. -De aanpak, tooling en risicoafwegingen bij OT-pentesten verschillen wezenlijk van IT-pentesten.	Dank voor uw suggestie om dit explicieter te benoemen. Pentesten op OT zijn inderdaad onderdeel van de scope van de raamovereenkomst.
20	3.1 CCV-keurmerk	15	Hoe wordt de kwaliteit van pentesters beoordeeld als zij niet beschikken over CCV-keurmerk, maar wel aantoonbare ervaring hebben?	Dit heeft samenhang met onze vraag P11 en P12. We staan nadrukkelijk open voor overige bruikbare criteria die op voldoende objectieve wijze onderscheidend vermogen en kwaliteitsbeheersing bieden zowel in een aanbesteding/minicompetitie, als in de uitvoering. Uw vraag aan ons is dus eigenlijk ook onze vraag aan de markt,
21	3.1 AI en QVC	16	In dit deel wordt AI en quantum cryptografie kort genoemd als opkomende ontwikkelingen. Is binnen de aanbesteding ruimte voor innovatieve testmethoden, zoals AI-ondersteunde pentests of quantum readiness scans en kunnen die als onderscheidend vermogen mogen worden ingebracht bij inschrijving of gunning?	Ja, in algemene zin zal bij elke aanvraag/opdracht (pentest) de ruimte hiervoor moeten blijken. Het is nog niet bepaald dat inschrijvers zich op deze onderwerpen kunnen onderscheiden in de aanbesteding voor de raamovereenkomst. In de aanbesteding zelf zult u dit terugzien.
22	3.1 Prijs	16	Er wordt verwacht dat we een fixed prijs offerte maken. Om dit te doen, hebben we een specifieke scope nodig. Kunt u specifieker zijn over de reikwijdte van de test (bijv. wat testen we, welke toegang krijgen we, enz.)	Deze vraag kunnen we in de context van deze marktraadpleging op het huidige generieke niveau niet verder duiden dan we hebben gedaan in de beschrijving, verwijzing naar methodieken en het concept PvE. U hoeft

Nr	Ref	Pag	Vraag	Antwoord
				voor deze marktraadpleging geen offerte in te dienen met een (vaste) prijs. We zoeken naar een prijsmodaliteit die volgens de respondenten in deze marktraadpleging het beste past voor afspraken in een raamovereenkomst en vele opdrachten daaronder. Wij begrijpen dat elke pentest een andere prijs zou kunnen hebben, maar moeten wel generieke afspraken in een raamovereenkomst vastleggen, die geldend zijn voor alle opdrachten daaronder maar wel ruimte geven voor de beste prijs voor een bepaalde pentest. Wat zou u ons adviseren? De vaste tijd en prijs is bedoeld gelezen te worden in relatie met ook vraag P7.
23	3.1 Nu/toekomst	17	De vragen hebben betrekking op een scope voor de komende 4 jaar. Verwacht u antwoorden op basis van de huidige situatie en mogelijkheden of verwacht u dat we rekening houden met toekomstige verwachtingen en mogelijkheden?	Beide, daar waar dat relevant is. Met betrekking tot AI en QVC zullen toekomstige verwachtingen een zwaardere rol hebben dan wellicht meer huidig al gebruikelijke aspecten. Dat is de expertise waarop we in deze marktraadpleging hopen en beroep op te mogen doen.
			Red teaming	
24	3.2	20	Met betrekking tot de Red Team-oefeningen: waar vinden deze plaats (Red Team-oefeningen zijn doorgaans oefeningen op locatie)? Zijn deze allemaal in Nederland of bijvoorbeeld ook de Antillen of andere locaties?	Red teaming via TIBER of ART vindt plaats in het kader van de digitale weerbaarheid binnen de afgesproken scope bij een Rijksoverheid organisatie. Waar de test precies op plaatsvindt is afhankelijk van het gekozen aanvalsscenario dat zal worden uitgevoerd en waarop de opdrachtgever akkoord geeft. Het gekozen scenario is gebaseerd op een dreigingsanalyse. Als uit de dreigingsanalyse blijkt dat fysieke aanwezigheid op locatie onderdeel is van het aanvalspatroon dan kan dat inderdaad onderdeel zijn van de test. In recente testen zien we echter dat de aanval voornamelijk binnen de digitale omgeving wordt uitgevoerd.
25	3.2 1.4 Doorlooptijd	20 7	Wat is de gemiddelde of gewenste doorlooptijd voor een Red Teaming opdracht. Mogen Opdrachtnemers een voorstel doen voor een gefaseerde aanpak (bijv. 8-10 weken), of zijn er vaste tijdskaders?	Voor red teaming wordt de TIBER en ART methodiek aangehouden. De doorlooptijd is afhankelijk van de gekozen methodiek en de modules daarbinnen (voor ART). Dit zal per RT-test kunnen verschillen, bijvoorbeeld afhankelijk van het aantal door de opdrachtgever gevraagde uit te voeren scenario’s, en onderdeel zijn van een plan van aanpak. Voor TIBER zijn er vaste kaders van 10 tot 12 weken doorlooptijd

Nr	Ref	Pag	Vraag	Antwoord
				voor de `actieve´ red team fase voor de uitvoering van de scenario's. Voor ART is dat afhankelijk van de gekozen modules en het aantal te spelen scenario's. Alle TIBER fases in totaal hebben een gemiddelde doorlooptijd 9 maanden tot soms wel een jaar, maar dat is inclusief de voorbereidingsfase (waaronder de aanbesteding), de testfase (waaronder TI-deelfase en RT-deelfase) en de afronding en leerfase (waaronder de purple teaming). Voor ART kan dat korter of langer zijn afhankelijk van het aantal gekozen modules.
26	3.2 Scope	20	Bij TIBER wordt de reikwijdte/scope bepaald door de TIP. Wat is uw verwachting van een vaste prijs als de scope niet vooraf is gedefinieerd?	De reikwijdte en scope worden in beginsel binnen TIBER en ART niet bepaald door de TIP. Het aantal te spelen scenario's en het gekozen raamwerk (inclusief modules) etc worden door de opdrachtgever al in de offerteaanvraag aan de voorkant gedefinieerd. De TIP zal op basis van het scoping document (waarin de opdrachtgever informatie over o.a. de kritieke functies van een organisatie verstrekt) potentiële dreigingsscenario's uitwerken in het TI-rapport. De opdrachtgever kiest vervolgens de scenario's die door de RTP in het testplan moeten worden uitgewerkt. Na een GO op het testplan kunnen de gekozen scenario's worden uitgevoerd in de actieve RT-fase. De opdrachtnemers kunnen een voorstel doen die past binnen de gevraagde raamwerken en gekozen modules.
27	3.2 Scope	21	Bij het onderdeel Pentesten geeft u aan dat Purple Teaming bij Red Teaming hoort, maar Purple Teaming wordt niet expliciet genoemd bij het onderdeel Red Teaming. Kunt u uitsluitsel geven of de dienstverlening Purple Teaming valt onder het onderdeel Red teaming?	Purple Teaming is onderdeel van de opdracht voor een ART/TIBER. Purple teaming in de afronding en leerfase maakt onderdeel uit van deze raamwerken. Van de opdrachtnemer wordt dienstverlening verwacht op het gebied van purple teaming conform de vereisten in ART en TIBER.
28	3.2 Type Red Teaming	21	Op pagina 21 geeft u aan "Deelnemende zelfstandige organisaties, zoals ZBO's, maken eigen afwegingen rond methodiek en uitvoering. Ook zij kunnen Red teaming testen volgens ART/TIBER, maar ook kiezen voor andere of lichtere vormen of smallere specifieke scope." Een ART kan, afhankelijk van de gekozen vorm, veel goedkoper zijn dan een TIBER. Heeft u bij het bepalen van het	Die verhouding hebben we niet concreet. De omvang van de behoefte buiten ART/TIBER evenmin. Vooralsnog richt de raamovereenkomst van RVICTO zich op ART/TIBER in lijn met de gekozen beleidsaanpak om red teaming via deze methodiek binnen de Rijksoverheid in te richten, conform een Tweede Kamer motie hierover in 2021.

Nr	Ref	Pag	Vraag	Antwoord
			budget, de verhouding tussen ART, TIBER en eventuele andere testen voor ogen gehad? Zo ja wat is daarvan de verhouding?	
29	3.2 RTP &/ TIP	22	Op pagina 23 geeft u aan: "In de praktijk is het voor de onafhankelijkheid goed als dit twee verschillend aangetrokken partijen zijn." Waar is deze aanname op gebaseerd? Inmiddels zijn er een aantal partijen in de markt die zowel TI als RT kunnen bieden en zeer zorgvuldig omgaan met de zgn. Chinese Walls. Op basis onze ervaring verdient dat zelfs de voorkeur aangezien goed op elkaar ingespeelde teams elkaar sneller begrijpen en er niet allerlei snijverlies optreedt in de overdracht. Wat is daarop uw reactie?	Twee verschillende partijen is meer concreet in onafhankelijkheid te duiden dan een set van afspraken. Dat doet niets af aan het feit dat beide varianten evenzeer van toegevoegde waarde kunnen zijn en geen van de varianten vooraf een voorkeur verdient. Het is een open keuze per voorgenomen RT-test naar de omstandigheden van dat geval. Er is geen aanleiding om in de aanbesteding van de raamovereenkomsten een variant boven de andere variant te stellen.
30	3.2 Beschikbaarheid	23	Op pagina 24 noemt u dat de beschikbaarheid van partijen bij een concrete aanvraag een aandachtspunt is. Dit is heel erg afhankelijk van de lead time of een eventuele planning die de opdrachtnemers kunnen inzien. Hoe lang is de periode voor de start van de beoogde test voordat de opdracht uitgezet wordt onder het raamwerk?	De planning voor red teaming testen binnen het Rijk kan niet worden gedeeld. De beoogde planning van een test is onderdeel van de offerteaanvraag. Het kan een voordeel zijn als een leverancier snel kan beginnen, maar het is ook mogelijk om in overleg de startdatum af te spreken met de opdrachtgever.
			SOC-diensten	
31	3.3	25	Wat is de scope (type en aantallen) van de applicaties die worden gemonitord?	Die informatie is niet beschikbaar en zal in hoofdzaak pas in nadere opdrachten aan de orde zijn. De omvang voor nu is uitgedrukt in de aantallen als vermeld. De opsplitsing van SOC-diensten in startpakket en aanvullende diensten is gedaan omdat we verwachten dat deelnemers van deze aanbesteding onderverdeeld kunnen worden in twee groepen. De eerste groep omvat deelnemers die beschikken over een algemeen gangbaar en generiek ICT-landschap. Type apparatuur die u hier aantreft zijn de in de markt gangbare ICT-werkplekken, communicatiemiddelen en kantoorautomatiseringsapplicaties. Voor deze groep

Nr	Ref	Pag	Vraag	Antwoord
				deelnemers verwachten wij dat te leveren monitoringdiensten met een relatief eenvoudige en standaard aanpak geïmplementeerd kan worden. Het startpakket beoogd om deze groep deelnemers op eenvoudige wijze te voorzien van gestandaardiseerde monitoringdiensten. De tweede groep zijn deelnemers met een meer complex landschap waarbij voor de implementatie een maatwerkaanpak is vereist. Deze deelnemers zullen naast het standaardpakket ook gebruik maken van aanvullende diensten. De componenttypen die u bij deze groep organisaties aantreft is zeer divers.
32	3.3.1 S12	26 34	Mogen opdrachtnemers eigen tooling inzetten (zoals SIEM, EDR, dashboards) en zijn er eisen voor koppeling met systemen van deelnemers? Dit is relevant voor interoperabiliteit, integratie en het benutten van bestaande platforms. Welke vrijheid hebben opdrachtnemers in het gebruik van eigen tooling, en zijn er eisen voor koppeling met systemen van de deelnemer?	Ja, u kunt eigen tooling inzetten. De eventuele eisen over koppelingen met systemen van de deelnemer kunnen per opdracht/deelnemer verschillen. Als aan de orde, zullen die in de aanvraag (minicompetitie) onder de raamovereenkomst vermeld worden.
33	3.3.5 E5 licenties	32	In het document wordt aangegeven dat diverse deelnemers beschikken over Microsoft E5-licenties en dat dit een voordeel kan zijn voor dienstverleners die met Microsoft-oplossingen werken. Kunt u toelichten in hoeverre ervaring met Microsoft E5-functionaliteiten (zoals Defender, Sentinel, etc.) een rol speelt in de beoordeling van inschrijvingen? Wordt dit als subgunningscriterium meegenomen, en zo ja, hoe wordt dit gewogen ten opzichte van leveranciers die met andere technologieën werken?	Op dit moment kan dat niet worden aangegeven. De achtergrond van deze vraag heeft minder betrekking op ervaring met producten die onder de Microsoft E5-licenties vallen. Met deze vraag wil aanbestedende dienst inzicht krijgen in de mogelijkheden en haalbaarheid om gebruik te maken van voorzieningen die reeds bij opdrachtgever aanwezig zijn. Biedt dit in uw ogen kansen of belemmeringen en zo ja, welke?
			Incident response	
34	3.4.1 Deelnemers IR	38	Om de scope en mogelijke omvang van de Incident Response/Forensisch Onderzoek (DFIR) uitvraag te kunnen inschatten, kunt u een indicatie geven van hoeveel deelnemers (Ministeries & ZBOs) er een afroep zouden kunnen doen vanuit het raamwerkcontract?	Zie het antwoord op vraag 3. De deelnemers zijn pas definitief deelnemer bij de aankondiging van de aanbesteding.

Nr	Ref	Pag	Vraag	Antwoord
			Omdat alle deelnemers van het raamwerkcontract onderhevig zijn onze risico-procedures, zouden we graag een lijst met alle deelnemers willen ontvangen zodat we de procedures alvast kunnen starten.	
35	3.4.1 Volwassenheid IR	38	Zijn er significante verschillen tussen de deelnemers (Ministeries & ZBO's) in algemene volwassenheid van de Incident Response & Forensisch Onderzoek? Bijvoorbeeld: is het waarschijnlijk dat enkele deelnemers wel IR "playbooks" en processen hebben gedocumenteerd en andere deelnemers niet?	Ja, die verschillen zullen er zijn, als ook in de mate waarin men en beroep op de markt doen of zou willen doen.
36	3.4.1 Opschaling IR		Is het voor de deelnemers (Ministeries & ZBOs) in het raamwerkcontract acceptabel dat in (significant) grotere incidenten kan worden opgeschaald met internationale collega's uit ons netwerk (Bijv uit: UK, USA, Ierland, Canada, Singapore, Duitsland, Frankrijk, Polen) die alleen Engels zouden spreken?	Ja, het is toegestaan internationale collega’s te betrekken, mits de verwerking van de data van deelnemers voldoet aan de door ons gestelde eisen en wetgeving hierover. M.b.t. taal: zie het antwoord 47 over de eisen A3 en A4 in Bijlage 1 Generieke Eisen. Tevens attenderen wij u op hoofdstuk 3, vraag A7 uit deze marktraadpleging.
37	3.4.1 Afname IR	38	Er wordt een onderscheid gemaakt van geheel of gedeeltelijke afname van IR-diensten (H3.3.1a-d). Is het doel in het raamwerk eenzelfde standaard set van IR diensten beschikbaar te stellen voor alle deelnemers?	Dat hangt ervan af of dat verstandig is. In de marktraadpleging onderscheiden we typen dienstverlening, zonder deze qua product los te zetten of in een geheel te vatten. We denken dat dit specifieke behoeften zijn die per deelnemer kunnen verschillen. Om de ondersteuning met raamovereenkomst optimaal te laten fungeren geloven we wel in een vooraf omschreven diensten/producten die voor alle deelnemers in ieder geval qua typering hetzelfde zijn. Concrete opdrachten moeten aansluit op de concrete situatie, dus zullen altijd ook casus-specifieke invulling hebben.
38	3.4.1 Type IR	38	Wordt de keuze voor type IR dienstverlening ("marktniveaus") gestandaardiseerd voor alle deelnemers in 1 raamwerkcontract of zou dit per deelnemer kunnen verschillen?	Deelnemers nemen IR af zoals hen dat past. Dat kan het geheel zijn van IR-dienstverlening of een of meer losse onderdelen.
39	3.4.1 BIO	38	Kunt u toelichten waarom BIO 2.0 niet als referentiekader is opgenomen in de uitvraag? En bent u voornemens dit alsnog te doen in het definitieve programma van eisen,	De verwijzing is naar de Baseline Informatiebeveiliging Overheid, ongeacht de geldende versie. Daarom wordt geen versie nummer genoemd.

Nr	Ref	Pag	Vraag	Antwoord
			zodat opdrachtnemers tijdig kunnen anticiperen op de nieuwe verplichtingen?	
			Cyber threat intelligence	
40	3.4.2 CTI	42	U heeft verschillende CTI-diensten uitgezet die vaak geïntegreerd zijn in één product. Denk aan een data feed en een meer generieke CTI-service. Waarom is hiervoor gekozen?	De diensten zijn als functioneel type geduid en zo product-onafhankelijk als mogelijk. Niettemin zijn we zeer gebaat bij een onderverdeling of pakketten zoals die in de markt regulier aangeboden worden om te bevragen.
41	3.4.2 CTI		Zoekt opdrachtgever ook naar actieve afstemming en een partnership om de TI bij deelnemers te beleggen en zo proactief de weerbaarheid te verhogen, bijvoorbeeld door het identificeren van specifieke (aanvullende) mitigatiemaatregelen voor deelnemers specifieke IT landschap? - Zo nee, identificeren wij dat CTI over het algemeen resulteert in datafeeds die onvoldoende actionable zijn voor de afnemers. Welke maatregelen neemt opdrachtgever om dit risico te adresseren, zijn hier specifieke partijen bij betrokken zoals wellicht het NCSC? - Zo ja, valt deze actieve afstemming binnen deelgebied 3.3.2.-d *Generieke/specifieke dreigingsbeelden* om zo proactief beveiligingsmaatregelen te verbeteren ("shift left")?	CTI is vooralsnog opgevat als leverancier van bepaalde type informatie al dan niet met specifiek bewerking. Deelnemers zijn de opdrachtgever van de nadere opdrachten. De indruk bestaat dat de dienstverlening waarin CTI gebruikt wordt al in de andere diensten een plek heeft. Zoals “het identificeren van specifieke (aanvullende) mitigatiemaatregelen voor deelnemers specifieke IT landschap” wat gelezen wordt als onderdeel van kwetsbaarheden (scans). Als er ene type CTI-dienst is die we onterecht over het hoofd zien, dan zien we die suggestie uiteraard graag tegemoet.
42	3.4.2-a Datafeed SOC	43	U vraagt bij de SOC-dienstverlening een dienst vanaf de plank uit. Moderne oplossingen, zoals managed automated detect en response diensten integreren vaak een CTI datafeed. Wat is het specifieke doel voor deze datafeed?	Het NCSC stelt een CTI-feed beschikbaar aan organisaties die tot de doelgroep behoren. De Rijksoverheid is zo’n doelgroep. Het NCSC kan via deze feed relevante informatie voor monitoringsystemen van betreffende doelgroep beschikbaar stellen. Op deze wijze kan het NCSC dreigingen die specifiek op een doelgroep van toepassing zijn geautomatiseerd beschikbaar stellen. Deze NCSC-feed is als aanvulling op reguliere CTI-datafeeds bedoeld en niet als vervanging.

Nr	Ref	Pag	Vraag	Antwoord
43	3.4.2-a Datafeed SOC	43	Hoe integreren de voorgestelde CTI-feeds en -diensten met bestaande beveiligingskaders en systemen die door de deelnemers worden gebruikt?	Als we de vraag goed begrijpen: dat zou elkaar niet in de weg hoeven staan. Op dit moment is geen sprake van bijzondere hindernissen vanuit systeem of beleid voor het gebruik van CTI-feeds.
44	3.4.2-a Datafeed SOC	43	Welke standaarden of benchmarks zullen worden gebruikt om de kwaliteit en betrouwbaarheid van de CTI-feeds te evalueren?	Dit is op dit moment nog niet bepaald of gekozen. Ideeën en inzichten kun u in deze marktraadpleging met ons delen.
			(Digitaal) Forensisch Onderzoek	
45	3.4.4 POB-nummer	47	Kunt u aangeven hoe het POB-nummer wordt ingebracht? En zou daadwerkelijke recherche werkzaamheden - indien vereist (maar normaliter zeer beperkt is de ervaring) - mogelijk door andere partijen kan worden verricht?	Uw eerste vraag is ons onvoldoende helder. U kunt uw POB-nummer bij uw eventuele inschrijving op de aanbesteding kenbaar maken. Het is mogelijk ook onderaannemers in te zetten voor recherchewerkzaamheden, maar ook zij zullen logischerwijs dan over een POB-nummer/vergunning moeten beschikken.
46	3.4.4 Opslag & retentie	47	Aangezien er mogelijk kosten bij data-opslag en retentie behoren; hebben de deelnemers zelf capaciteiten voor opslag en retentie van forensische artifacten?	Die mogelijkheid kan per opdracht/deelnemer afgestemd worden.
			BIJLAGE 1 PVE-CPT GENERIEKE EISEN	
47	A3, A4 Taal	2	Vraag over Bijlage 1, pagina Eisen A3 en A4 (Taal). De opdrachtgever vraagt hier op voorhand om de Nederlandse taal zowel als het gaat om documenten als om de inzet van het in te zetten personeel, tenzij expliciet anders aangegeven. Wij zijn een wereldwijd opererende organisatie en onze kracht om effectief klanten te kunnen ondersteunen op het gebied van informatiebeveiliging halen we juist uit onze wereldwijde kennis, kunde en actuele inzichten. Dreigingen houden immers niet op bij onze landsgrenzen. Door een dergelijk stringente taaleis beperkt u zich in de rechtstreekse toegang tot de wereldwijde community op het gebied van	De mogelijkheid een andere taal dan Nederlands in te zetten, kan per opdracht met de opdrachtgever afgestemd worden en verschillen. Ook binnen een opdracht kan hierbij nog onderscheid gemaakt worden tussen de verschillende doelen en middelen van communicatie (informeel/formeel, welke doelgroepen etc.) en de opdracht-specifieke risico’s bij gebruik van een andere taal dan het Nederlands. Het is bijvoorbeeld denkbaar dat met buitenlandse collega’s in het Engels wordt gecommuniceerd, maar dat (formele)documentatie (ook) in het Nederlands opgesteld wordt.

Nr	Ref	Pag	Vraag	Antwoord
			informatiebeveiligingsdiensten. Is de opdrachtgever bereid om op voorhand deze taaleis te verbreden naar een situatie waarin alle contractuele zaken (NOK) in het Nederlands gebeuren (zowel taal als personeel) maar waar de uitvoering van diensten ook in het Engels (documenten en in te zetten personeel) mogelijk is?	Er is nu gekozen voor 'Nederlands, tenzij', omdat deze keuze overeenkomt met de praktijk bij de diverse deelnemers.
48	A3, A4 Taal	2	Onze vraag ziet op de mogelijkheid om met een tweetalige opzet te werken: Nederlandstalige frontoffice voor communicatie en rapportage, gecombineerd met een internationaal backoffice-team voor uitvoering. Dit stelt ons in staat om kwaliteit en schaalbaarheid te combineren met kostenefficiëntie In de marktraadpleging wordt aangegeven dat Nederlands de voertaal is bij de deelnemers. Kunt u toelichten in hoeverre dit een harde eis is voor alle onderdelen van de dienstverlening (zoals rapportages, communicatie tijdens uitvoering, intakegesprekken, etc.)? Is het bijvoorbeeld toegestaan om met een tweetalige opzet te werken, waarbij Nederlandstalige frontoffice-consultants optreden als aanspreekpunt voor de deelnemer, terwijl de uitvoering (bijv. pentesten) door een internationaal backoffice-team wordt verzorgd?	Zie antwoord 47. Uw voorstel is in algemene zin denkbaar, maar dit zal echt per opdracht afgestemd moeten worden. Naast communicatierisico's kunnen er ook veiligheidsrisico's verbonden zijn aan uw voorstel.
			BIJLAGE 2 PVE-CPT PENTESTEN	
49	B2.10	2	Opdrachtgever geeft aan dat de intake niet bedoeld is om de scope wezenlijk te wijzigen. Kan de Opdrachtgever toelichten hoe wordt omgegaan met wijzigingen die noodzakelijk blijken tijdens de intake (bijvoorbeeld omdat de oorspronkelijke scope technisch onhaalbaar blijkt binnen de tijd)?	Beoogd is dat dergelijke obstakels duidelijk worden voordat opdrachtnemers (binnen de raamovereenkomst) een offerte indienen. Een wezenlijke wijziging van de opdracht moet voorkomen worden, maar er moet enige ruimte zijn voor het omgaan met (on)voorziene situaties of risico's in de uitvoering van de opdracht. Risico's zullen zoveel als mogelijk bij de intake en in het plan van aanpak besproken en verwerkt moeten worden.
50	B2.12	2	Wordt er een voorgeschreven format aangeleverd voor het verslag van het intakegesprek, of is dit ter discretie van	Nee, een format voor (verslag van het) intakegesprek wordt niet voorzien. Aanbestedende dienst overweegt een format

Nr	Ref	Pag	Vraag	Antwoord
			opdrachtnemer zolang de genoemde elementen worden opgenomen?	voor het plan van aanpak op te stellen, als er bredere behoefte aan een dergelijke standaard is.
51	B2.15 B2.28	2 5	Indien tijdens de intake scopewijzigingen worden overeengekomen, kan de accordering dan plaatsvinden in een bijgewerkt plan van aanpak? Of moet hiervoor een aparte bevestiging via een wijzigingsformulier of bijlage plaatsvinden?	Een beperkte scopewijziging kan verwerkt worden in het plan van aanpak, dat door beide partijen goedgekeurd moet worden. Een wezenlijke wijziging van de scope zal moeten leiden tot een nieuwe minicompetitie.