Nota van Inlichtingen Marktconsultatie Incident Response Retainer diensten

Nr.	Document / Bijlage / Onderwerp	Pagina	Paragraaf / Eis	Vragen / Opmerkingen	Antwoord
Vraag ID	*Het betreffende document, bijlage of onderwerp van de vraag*	*Het paginanummer waar de vraag betrekking op heeft.*	*Nummer waaronder de eis of wens in het beschrijvend staat opgenomen*	*Hier kunt u uw vraag stellen.*	*Hier vult de aanbestedende dienst het definitieve antwoord in.*
0					Algemeen: De Belastingdienst merkt op dat veel van de vragen van vragenstellers over de inhoud, scope en mogelijke omvang gaan. Hoewel de Belastingdienst deze vragen begrijpt en deze zo goed mogelijk tracht te beantwoorden, geeft zij graag mee dat deze informatie in dit stadium nog niet te geven is, en deels niet nodig is. Het doel van deze marktconsultatie is inzicht te verkrijgen in de diensten die de markt op dit gebied kan leveren evenals de kwaliteit, specificaties, details en toegevoegde waarde ervan voor de Belastingdienst. Op het moment van aanbesteding zal alle informatie omtrent de scope (mogelijke soorten incidenten), omvang, reikwijdte etc. welke voor inschrijvers nodig is om een passende inschrijving te kunnen doen, onder non disclosure beschikbaar worden gesteld

1				Als internationale cybersecuritydienstverlener zetten wij, afhankelijk van de casus, specialistische incident response-capaciteit vanuit meerdere Europese landen in. Zijn er op dit moment al uitgangspunten bekend voor de geografische locatie van incident responders en de verwerking en opslag van onderzoeksgegevens? Dit helpt ons om onze mogelijkheden en werkwijze passend te beschrijven in de reactie op deze marktconsultatie.	Ja er zijn qua geografische locatie van incident responders en de verwerking en opslag van onderzoeksgegevens een aantal zaken die belangrijk zijn: - minimale aanrijdtijd in geval van een incident waar de IRR dienstverlening is benodigd - voorkomen van risico's op het vlak van digitale autonomie en digitale soeveriniteit. Ten aanzien van de IRR diensten is een situatie denkbaar dat de opdrachtnemer zelf, dan wel toeleveranciers, door een machtspositie van een bepaalde entiteit tijdens de looptijd van het contract: * de bij Opdrachtnemer beschikbare vertrouwelijke (Persoons)Gegevens kan opvragen/zich eigen kan maken, terwijl Belastingdienst daar geen toestemming voor heeft gegeven; * het gebruik van de IRR diensten aan de Belastingdienst op enig moment kan worden ontzegd dan wel beperkt.
2				Is de beoogde dienstverlening primair een aanvulling op het eigen CSIRT en de bestaande beheerteams, of wordt ook zelfstandige uitvoering van respons- en herstelmaatregelen verkend? Staat de Belastingdienst daarbij open voor het inzetten van specialistische partners voor onderdelen van de dienstverlening, bijvoorbeeld voor onderhandelingen met dreigingsactoren bij ransomware of afpersing en het eventueel faciliteren van losgeldbetalingen?	De IRR diensten zijn in eerste instantie een aanvulling op de reeds ingerichte CSIRT en bestaande kennis en kunde. Indien met specialistische partners onderaannemers van opdrachtnemer worden bedoeld dan is het antwoord in principe Ja. Voorwaard is dat opdrachtnemer verantwoordelijk is en blijft en de overeengekomen kwaliteit van de opdracht, bijvoorbeeld m.b.t. de informatiebeveiliging, niet in het geding komt.

3				Kan de Belastingdienst de indicatieve omvang van de te ondersteunen omgeving en de betrokken organisaties nader toelichten? Moeten de inzetgebieden in bijlage 1 worden gelezen als mogelijke toepassingsgebieden of als beoogde integrale dekking?	In bijlage 1 staan de mogelijke inzetgebieden waarvoor de IRR diensten bij de Belastingdienst kunnen spelen. Voor een beschrijving van de organisatie zie paragraaf 1.3 van het marktconsultatiedocument.
4				Kunt u aangeven wat u verstaat onder juridisch houdbare verslaglegging en bewijsvoering in vraag 30?	Indien de IRR diensten leiden tot opsporing en vervolging van verdachte personen of organisaties zal het openbaar ministerie gebruik moeten kunnen maken van ter zake relevante informatie die bij de IRR diensten is vastgelegd
5				Kan Opdrachtgever inzicht geven in het aantal, de aard en de omvang van incidenten waarvoor de afgelopen jaren externe incidentrespons nodig was, en in de verwachte behoefte voor de komende jaren? Deze informatie helpt potentiële inschrijver om een passend retainer-model en de benodigde capaciteit te bepalen.	De informatie is vertrouwelijk van aard en wordt niet openbaar gemaakt daarbij is deze informatie is in dit stadium nog niet nodig. Zie de algemene opmerking van de Belastingdienst.

6				In §4.4 van het marktconsultatiedocument staat 30 oktober 2026 als uiterste datum voor de inhoudelijke beantwoording, terwijl de aankondiging 14 oktober 2026 om 23.59 uur noemt als “Termijn ontvangst antwoorden”. Kan Opdrachtgever bevestigen welke datum geldt en wat de exacte sluitingstijd is? Kan opdrachtgever tevens bevestigen dat vragen die uiterlijk 7 oktober om 12.00 uur worden ingediend, worden beantwoord in de Nota van Inlichtingen van 14 oktober?	Voor de beantwoording van de marktconsultatievragen geldt de planning uit paragraaf 4.4 van het marktconsultatiedocument: de beantwoording dient uiterlijk 30 oktober 2026 om 12:00 uur te zijn ingediend via de daartoe bestemde module in TenderNed.
7				Kan Opdrachtgever aangeven welke incidentresponsactiviteiten het eigen CSIRT momenteel uitvoert en voor welke activiteiten inzet wordt verwacht of regie van de retainerleverancier? Welke bevoegdheden wenst Opdrachtgever de toekosmtige leverancier te geven bij onderzoek, containment en herstel?	Het eigen CSIRT voert in voorkomende situaties alle IRR activiteiten zelfstandig uit. IRR dienstverleners hebben voornamelijk toegevoegde waarde ophet gebied van - regie (objectief en los van interne emotie), - snel kunnen leveren van extra kundige menskracht, - extern niet gecompromitteerde forensische capaciteit (mensen en middelen) - onderhandelingen (mocht bevoegd gezag daartoe besluiten uiteraard).

8				Kan Opdrachtgever aangeven naar welke 'activiteiten binnen een breed terrein' zij verwijst met betrekking tot het bestaande SOC? Kan Opdrachtgever inzicht geven in de toekomstige ziet rolverdeling tussen het SOC en de toekomstige IRR-leverancier waarbij zij o.a. specifiek ingaat op het aspect threat intelligence?	Zie het antwoord op vraag 7.
9				Welke verwachtingen heeft Opdrachtgever ten aanzien van 24/7-beschikbaarheid, responstijden en capaciteit bij omvangrijke of gelijktijdige incidenten? Welk indicatief incidentvolume kan worden gebruikt bij het beschrijven van een passend retainermodel?	Dat is moeilijk aan te geven. Wellicht kan gegadigde dit ischatten op basis van de aard van de organisatie (zie paragraaf 1.3 van het marktconsultatiedocument) en de eigen ervaring met IRR diensten voor een vergelijkbare partij. Zie de algemene opmerking van de Belastingdienst.
10				Welke activiteiten hebben voor Opdrachtgever de hoogste prioriteit wanneer geen incident plaatsvindt, bijvoorbeeld threat hunting, forensic readiness, oefeningen of kennisoverdracht?	Activiteiten welke zijn gericht op het voorkomen van de inzet van een IRR dienstverlener, daarna activiteiten op het beperken van eventuele schade van onderhavige incidenten
11				Kan Opdrachtgever bevestigen dat het beheren van omgevingen buiten de scope van desbetreffende toekomstige aanbestding zal vallen?	Het beheren van de ICT-idiensten blijft een verantwoordelijkheid van de Belastingdienst

12				Op pagina 10 van desbetreffende marktconsultatie noemt Opdrachtgever dat zij "voornemens is op termijn IR-diensten te verwerven." Kan Opdrcahtgever een indicatie geven van de gewenste startdatum van deze diensten?	De marktconsultatie is een voorbereiding op een mogelijke verwerving. De Belastingdienst is voornemens op termijn Incident Response Retainer diensten te verwerven. De gewenste startdatum is nog niet vastgesteld, mede omdat deze afhangt van de opdrachtstrategie en de uitkomsten van deze marktconsultatie. De Belastingdienst kan daarom op dit moment geen indicatie geven.

13				Op pagina 11 van desbetreffende marktconsultatie stelt Opdrachtgever o.a. de vraag over een "recente ISO27001 certificering of minimaal daarmee vergelijkbaar information security managent system". Kan Opdrachtgever bevestigen dat een SOC II type 2 verklaring volstaat in plaats van een ISO27001 certificering? Inschrijver merkt op dat een SOC 2 Type II-rapportage een zwaardere en diepgaandere toets op de werking van beheersmaatregelen over een referentieperiode dan een momentopname-certificering. Kunt u, mede gelet op het proportionaliteits- en gelijkwaardigheidsbeginsel, bevestigen dat een geldige SOC 2 Type II-rapportage, als gelijkwaardig bewijs van aantoonbaar ingerichte en werkende informatiebeveiligingsmaatregelen wordt geaccepteerd? Zo nee, kunt u gemotiveerd toelichten waarom een aantoonbaar zwaardere assurance op de werking van controls in dit geval niet als gelijkwaardig bewijs kan gelden ten aanzien van desbetreffende martkconsultatie?	Waar ISO 27001 een officieel certificaat oplevert voor een managementsysteem is SOC 2 Type II een assurancerapport dat de werking van specifieke beveiligingsmaatregelen over een periode aantoont.

14				Inschrijver merkt op dat in pagina 16 van de marktconsultatie m.b.t. de voertaal het navolgende is opgenomen "voertaal tijdens deze marktconsultatie is Nederlands, productinformatie mag in het Engels". Kan Opdrachtgever bevestigen dat m.b.t. de uitvoering van Incident Response en de gewenste nevenactiviteiten, Engelstalige communicatie en rapportage eveneens is toegestaan mits Nederlands de boventoon voert (voor o.a. managementsamenvattingen) en voldaan is aan alle andere vereisten. Dit betreft met name technische apspecten.	Nee de Belastingdienst kan dit niet bevestigen.
15				Kan Opdrachtgever aangeven welke organisaties en technische omgevingen bij aanvang onder de toekomstige IRR-dienstverlening zullen vallen? Kan Opdrachtgever daarbij inzicht geven in welke van de in de marktconsultatie genoemde infrastructuurdomeinen zij wenst daadwerkelijk binnen de scope te doen laten vallen, de belangrijkste gebruikte platformen en de indicatieve omvang daarvan? Deze informatie helpt potentiële inschrijver om de benodigde expertise en capaciteit te bepalen.	Zie het antwoord op vraag 3 en de algemene opmerking van de Belastingdienst.

16				Op pagina 12 van de marktconsultatie vraagt Opdrachtgever naar de mogelijkheden om grote hoeveelheden gegevens naar een veilige onderzoeksomgeving van de leverancier te transporteren. Kan Opdrachtgever aangeven of het gebruik van een cloudgebaseerde forensische onderzoeksomgeving is toegestaan? Welke voorwaarden gelden daarbij ten aanzien van gegevensclassificatie, opslag- en verwerkingslocatie, toegang vanuit het buitenland, bewaartermijnen en verwijdering van onderzoeksgegevens?	Cloudaspecten in de IRR dienstverlening zijn in principe niet uitgesloten. Een DPIA zal onderdeel van de verwerving worden. Alle Gegevens van Opdrachtgever zijn ten minste van het niveau Departementaal Vertrouwelijk (DepV). Zie ook antwoord op vraag 1.
17				In §3.13 van de marktconsultatie geeft Opdrachtgever aan ook in perioden zonder incidenten maximaal toegevoegde waarde uit de retainer te willen ontvangen. Kan Opdrachtgever aangeven of zij openstaat voor een model waarbij vooruitbetaalde uren of budget kunnen worden ingezet voor vooraf overeengekomen weerbaarheidsactiviteiten en gedeeltelijk kunnen worden overgedragen naar een volgend contractjaar? Kan Opdrachtgever tevens aangeven of, na besteding van dit budget, aanvullende incidentrespons kan worden uitgevoerd tegen vooraf overeengekomen tarieven?	De Belastingdienst staat open voor aanvullende voorstellen en alternatieve invullingen (hoofdstuk 3). Het voorgestelde model, met vooruitbetaalde uren of budget voor vooraf overeengekomen weerbaarheidsactiviteiten, gedeeltelijke overdracht naar een volgend contractjaar en additionele incidentrespons tegen vooraf overeengekomen tarieven, kan worden meegenomen in de beantwoording van vraag 40 en 41, inclusief voor- en nadelen. Er kunnen geen toezeggingen worden gedaan over de uiteindelijke vormgeving van het afrekenmodel. De Belastingdienst is niet gebonden aan de uitkomsten van de marktconsultatie.

18	Aansprakelijkheid		Hoofdstuk 4 / toekomstige contractvoorwaarden	Wij vragen de Belastingdienst expliciet aandacht te besteden aan de aansprakelijkheids- en vrijwaringsbepalingen in de definitieve uitvraag. Incident Response dienstverlening kent een wezenlijk ander risicoprofiel dan reguliere ICT-dienstverlening, omdat werkzaamheden plaatsvinden tijdens beveiligingsincidenten waarbij de oorzaak, omvang en impact van het incident vaak nog niet volledig bekend zijn. Een onbegrensde of voor reguliere dienstverlening ontworpen risicoverdeling kan daardoor disproportioneel uitpakken voor leveranciers. Wij vernemen graag of de Belastingdienst bereid is hiermee rekening te houden bij de formulering van de contractvoorwaarden.	Deze marktconsultatie maakt geen deel uit van de aanbesteding en de contractvoorwaarden zijn nog niet vastgesteld. De Belastingdienst heeft kennisgenomen van de opmerking over het risicoprofiel van incident response dienstverlening en zal deze betrekken bij haar overwegingen over het opstellen van de contractvoorwaarden.
19	Incidentvolume en gelijktijdigheid		Hoofdstuk 3 – organisatie, capaciteit en beschikbaarheid	Kan de Belastingdienst inzicht geven in het verwachte aantal incidenten per jaar, het historische gebruik van vergelijkbare dienstverlening en de verwachte situatie wanneer meerdere incidenten gelijktijdig ondersteuning vereisen?	Zie het antwoord op vraag 5.

20	Scope afnemers		Hoofdstuk 2 – scope van de dienstverlening	Is de Belastingdienst voornemens de toekomstige overeenkomst uitsluitend beschikbaar te stellen aan de Belastingdienst zelf, of ook aan andere organisatieonderdelen en afnemers binnen het domein waarvoor de dienstverlening relevant kan zijn? Zo ja, welke onderdelen en afnemers vallen naar verwachting binnen de scope?	Zie het antwoord op vraag 3.
21	Rolverdeling tijdens incidenten		Hoofdstuk 3 – samenwerking met CSIRT en overige leveranciers	Welke rol ziet de Belastingdienst voor de toekomstige Incident Response-partner ten opzichte van het interne CSIRT, bestaande SOC-dienstverlening en overige security- en IT-leveranciers tijdens een actief incident?	Zie het antwoord op vraag 7.
22	Retainermodel		Hoofdstuk 3 – retainer-dienstverlening en afrekenmodellen	Heeft de Belastingdienst op dit moment een voorkeur voor een beschikbaarheidsretainer, een prepaid budget, inzet op nacalculatie of een hybride constructie, of beschouwt de Belastingdienst de keuze voor het meest passende model nadrukkelijk als uitkomst van deze marktconsultatie?	De Belastingdienst heeft op dit moment geen vastgestelde voorkeur voor een bepaald retainer- of afrekenmodel. De keuze voor het meest passende model is nadrukkelijk een uitkomst van deze marktconsultatie. Marktpartijen worden uitgenodigd de verschillende modellen en hun voor- en nadelen te beschrijven bij vraag 40 en 41.

23	Forensische data en datalocatie		Hoofdstuk 3 – forensisch onderzoek en informatiebeveiliging	Zijn er specifieke eisen of randvoorwaarden ten aanzien van de opslaglocatie, overdracht, verwerking en analyse van forensische onderzoeksdata, bijvoorbeeld met betrekking tot Nederlandse of Europese datalocaties, maximale datavolumes of werkzaamheden op locatie?	Zie het antwoord op vraag 16.
24	Screening en toegangsmachtigingen		Hoofdstuk 3 – informatiebeveiliging en inzet van personeel	Verwacht de Belastingdienst dat medewerkers van de toekomstige Incident Response-partner beschikken over specifieke screenings, veiligheidsonderzoeken of aanvullende toegangsmachtigingen? Zo ja, welke eisen en doorlooptijden voorziet de Belastingdienst?	Zie de algemene opmerking van de Belastingdienst.

25	Referenties en referentiebezoeken		Hoofdstuk 3.1 Organisatie en ervaring (vraag 7)	De Belastingdienst vraagt in de marktconsultatie naar de mogelijkheid van referentiebezoeken. Incident Response-dienstverlening kent echter een vertrouwelijk karakter, waardoor referenties en casuïstiek niet altijd openbaar gedeeld kunnen worden. Kan de Belastingdienst aangeven welke rol referenties en referentiebezoeken naar verwachting gaan spelen binnen een eventuele toekomstige aanbesteding? Daarnaast vernemen wij graag of geanonimiseerde referenties, referentieverklaringen of alternatieve vormen van aantoonbare ervaring eveneens als passend bewijs van ervaring worden beschouwd.	De rol van referenties in een eventuele aanbesteding is nog niet vastgesteld. Eventuele geschiktheidseisen worden proportioneel opgesteld en komen in de aanbestedingsdocumenten. Vraag 7 is in het kader van de marktconsultatie gesteld. De Belastingdienst erkent het vertrouwelijke karakter van incident response diensten en zal hiermee rekening houden bij het bepalen van het bewijs dat wordt gevraagd. Geanonimiseerde referenties en alternatieve vormen van aantoonbare ervaring kunnen daarbij worden overwogen.
26	Marktconsultatie Incident Response Retainer diensten.pdf	8	Paragraaf 1.3.5	Paragraaf 1.3.5 vermeldt dat de retainer in eerste instantie voor de Belastingdienst wordt ingezet, maar ook beschikbaar kan komen voor andere organisaties die DCS-diensten afnemen; voetnoot 5 noemt ook overheidsorganisaties buiten de rijksoverheid. Kunnen deze organisaties zelfstandig een beroep doen op de toekomstige retainer, en vallen zij dan onder dezelfde retainer en voorwaarden?	De IIR diensten die hier aan de orde zijn betreffen de ICT-diensten die vanuit het ODC-BD beschikbaar worden gesteld. In voorkomende gevallen maken andere (rijks)overheden voor hun bedrijfsprocessen gebruik van deze ICT-diensten. Deze kunnen niet zelfstandig een beroep doen op de IRR dienstverlener. DCS is verantwoordelijk voor de beschikbaarstelling van deze ICT-diensten.

27	Marktconsultatie Incident Response Retainer diensten.pdf	10, 11, 12, 13	hoofdstuk 3	Hoofdstuk 3 inventariseert uiteenlopende retainerdiensten als basis voor de latere opdrachtstrategie, van forensisch onderzoek en technische respons tot crisismanagement. Kunt u aangeven welke richting de Belastingdienst onderzoekt: één geïntegreerde opdracht of afzonderlijke percelen of dienstpakketten, bijvoorbeeld voor forensisch onderzoek, incidentrespons en crisismanagement?	De belastingdienst heeft nog niet besloten of de opdracht integraal of in percelen wordt aanbesteed. Hoofdstuk 3 is bedoeld als brede inventarisatie en vormt input voor de verwervingsstrategie. Marktpartijen kunnen in hun reactie aangeven welke inrichting zij het meest passend vinden, inclusief de voor en nadelen daarvan.
28	Marktconsultatie Incident Response Retainer diensten.pdf	10, 17	hoofdstuk 3	Bijlage 1 noemt inzetgebieden voor IR-retainerdiensten en hoofdstuk 3 beschrijft de onderwerpen als een brede inventarisatie. Moeten wij bijlage 1 lezen als voorbeelden van mogelijke inzet, of als de beoogde inhoudelijke afbakening van de toekomstige opdracht?	Zie het antwoord op vraag 3.
29	Marktconsultatie Incident Response Retainer diensten.pdf	13, 15	paragraaf 4.6	Vraag 41 vraagt naar alternatieve afrekenmodellen en hun voor- en nadelen; paragraaf 4.6 sluit offertes uit. Verwacht u bij de beantwoording van vraag 41 uitsluitend een kwalitatieve beschrijving, of ook indicatieve bedragen of prijsopbouw?	Een kwalitatieve beschrijving van de afrekenmodellen en de prijselementen inclusief de voor- en nadelen volstaat. Er worden geen offertes of concrete tarieven gevraagd maar het staat deelnemers vrij een indicatie van de orde van grootte te geven als dit helpt bij de toelichting.

30	Marktconsultatie Incident Response Retainer diensten.pdf	14, 15, 16	Paragraaf 4.3, paragraaf 4.7	Paragraaf 4.3 en randvoorwaarde 10 van paragraaf 4.7 beschrijven vertrouwelijke behandeling en geanonimiseerde verwerking, terwijl randvoorwaarde 12 vrij gebruik toestaat. Kunt u aangeven hoe product-, methode- en bedrijfsgevoelige details uit reacties worden behandeld wanneer de uitkomsten worden gedeeld of verwerkt?	De inbreng van deelnemers wordt zoveel mogelijk vertrouwelijk behandeld (paragraaf 4.3 en randvoorwaarde 8). Resultaten kunnen worden verwerkt in aanbestedingsdocumenten of openbaar worden gemaakt zonder dat deze herleidbaar zijn tot deelnemers (randvoorwaarde 6 en 12). Bedrijfsgevoelige details worden daarbij niet herleidbaar gemaakt of gedeeld.
31	Marktconsultatie Incident Response Retainer diensten.pdf	14	Paragraaf 4.4	Paragraaf 4.4 vermeldt 30 oktober 2026 als uiterste moment voor het insturen van de beantwoording, zonder tijdstip. Welk tijdstip geldt die dag als sluitingstijd voor indiening via TenderNed?	Ziet het antwoord op vraag 6.
32	Marktconsultatie Incident Response Retainer diensten.pdf	14, 15	Paragraaf 4.5	Paragrafen 4.4 en 4.5 noemen een mogelijk mondeling vervolg van begin tot medio november. Welke duur en opzet voorziet de Belastingdienst voor een eventuele toelichtingsbijeenkomst, zodat deelnemers de benodigde voorbereiding en capaciteit kunnen plannen?	Eventuele toelichtingsbijeenkomsten vinden plaats per deelnemer in de periode begin tot medio november 2026. De opzet en duur worden bij de uitnodiging bekendgemaakt.
33	Marktconsultatie Incident Response Retainer diensten.pdf	15	Paragraaf 4.5	Paragraaf 4.5 vermeldt dat deelnemers mogelijk worden uitgenodigd voor een schriftelijke toelichting of aanvullende bijeenkomst. Kunt u aangeven hoe wordt bepaald welke deelnemers worden uitgenodigd en of alle deelnemers daarvoor in aanmerking komen?	De Belastingdienst bepaalt op basis van de ontvangen reacties welke deelnemers worden uitgenodigd voor een toelichting. Dat kan inhouden dat alle deelnemers worden uitgenodigd. Een uitnodiging, of het ontbreken daarvan, heeft geen gevolgen voor deelname aan een eventuele aanbesteding en levert geen voorrangspositie of uitsluiting op.

34	Marktconsultatie Incident Response Retainer diensten.pdf	7	Paragraaf 1.3.4	DCS heeft een eigen Security Operations Center en de Belastingdienst een eigen CSIRT. Op welk moment gaat een incident in de beoogde situatie over van het eigen SOC naar de IR-retainerpartij? Valt continue detectie (MDR) door de retainerpartij binnen de scope, of blijft die nadrukkelijk buiten de opdracht?	Zie het antwoord op vraag 7. MDR valt niet binnen de scope van IRR diensten, maar is een activiteit die binnen de SOC diensten valt.
35	Marktconsultatie Incident Response Retainer diensten.pdf	8	Paragraaf 1.3.4	In het organogram van DCS staat bij Klantspecifieke Diensten een 'Forensisch Domein'. Hoe verhoudt de gevraagde forensische dienstverlening zich tot deze interne capaciteit: als aanvulling, als opschaling bij grote incidenten of als vervanging?	Het forensisch domein betreft ICT-diensten die uitsluitend beschikbaar worden gesteld voor de FIOD (Fiscale Inlichtingen- en Opsporingsdienst) als onderdeel van de Belastingdienst (https://www.fiod.nl/). Het forensich domein wordt in principe niet ingezet ten behoeve van de IRR diensten of CSIRT activiteiten.
36	Marktconsultatie Incident Response Retainer diensten.pdf	8, 17-21	Bijlage 1	Het organogram van DCS noemt twee mainframe-hostingomgevingen. Bijlage 1 noemt mainframes niet als inzetgebied. Valt incident response op mainframe-omgevingen binnen de beoogde scope?	De mainframe omgeving valt in bijlage 1 onder servers en besturingssystemen en valt binnen de scope.
37	Marktconsultatie Incident Response Retainer diensten.pdf	11	Hoofdstuk 3, vraag 10	Welke screeningseisen overweegt u voor in te zetten medewerkers, bijvoorbeeld een VOG of een veiligheidsonderzoek voor vertrouwensfuncties? En met welk rubriceringsniveau van informatie verwacht u dat IR-medewerkers tijdens een incident te maken krijgen?	Zie de algemene opmerking van de Belastingdienst.

38	Marktconsultatie Incident Response Retainer diensten.pdf	11	Hoofdstuk 3, vraag 4	Overweegt u eisen aan de locatie van waaruit de dienstverlening wordt geleverd, of aan de vestigingsplaats van in te zetten medewerkers? Kan bij een groot of langdurig incident capaciteit uit andere EU-lidstaten worden ingezet, mits die medewerkers aan dezelfde screeningseisen voldoen?	Zie het antwoord op vraag 1.
39	Marktconsultatie Incident Response Retainer diensten.pdf	12	Hoofdstuk 3, vraag 21	Vraag 21 gaat uit van transport van gegevens naar de omgeving van de leverancier. Welke eisen overweegt u aan de locatie en jurisdictie van die omgeving, bijvoorbeeld opslag en verwerking uitsluitend binnen de EU, of uitsluiting van partijen die onder niet-EU-wetgeving zoals de US CLOUD Act vallen? Is onderzoek op locatie of binnen de eigen omgeving van de Belastingdienst ook een optie?	Zie het antwoord op vraag 16. Onderzoek op locatie of binnen de eigen omgeving van de Belastingdienst is een optie
40	Marktconsultatie Incident Response Retainer diensten.pdf	41579	Hoofdstuk 3	Verwacht u dat de retainerpartij bij een incident vooral werkt met de EDR/XDR- en SIEM-tooling die al aanwezig is? Of mag de leverancier eigen forensische tooling en agents uitrollen, en welke goedkeuringsprocedure geldt daarvoor binnen de rijksomgeving?	In beginsel niet. Maar er zouden situaties kunnen ontstaan wanneer dit noodzakelijk wordt geacht.

41	Marktconsultatie Incident Response Retainer diensten.pdf	11	Hoofdstuk 3, vraag 9 en 12	Aan welke responstijden denkt u voor remote inzet en voor inzet op locatie? Gaat het bij inzet op locatie vooral om de datacenterlocaties, of ook om andere vestigingen van de Belastingdienst, Douane en Toeslagen?	Remote inzet onmiddellijk, inzet op locatie binnen 2 uren, het betreft datacenterlocaties.
42	Marktconsultatie Incident Response Retainer diensten.pdf	10	Hoofdstuk 2	Kunt u een indicatie geven van het aantal incidenten per jaar waarvoor u externe inzet verwacht, en van de beoogde contractduur? Dat helpt ons om bij vraag 40 en 41 realistische afrekenmodellen te schetsen.	Zie het antwoord op vraag 5.
43	Marktconsultatie Incident Response Retainer diensten.pdf	11	Hoofdstuk 3, vraag 10	Overweegt u naast ISO 27001 nog andere eisen, zoals aantoonbare BIO-conformiteit, CREST-accreditatie, ISO/IEC 17025 voor forensisch onderzoek of persoonsgebonden certificeringen? Staat u open voor aantoonbaar gelijkwaardige alternatieven?	Aantoonbaar gelijkwaardige alternatieven zijn toegestaan.
44	Marktconsultatie Incident Response Retainer diensten.pdf	16	Paragraaf 4.7, randvoorwaarde 9	Moeten rapportages en communicatie tijdens een incident in het Nederlands, of is Engels toegestaan voor technische forensische rapportages?	Zie het antwoord op vraag 14.

45	Marktconsultatie Incident Response Retainer diensten.pdf	12	Hoofdstuk 3, vraag 23	Hoe kijkt de Belastingdienst als overheidsorganisatie aan tegen onderhandelen met dreigingsactoren? Hoort dit bij de beoogde dienstverlening, of beperkt de rol van de leverancier zich tot advies en dreigingsinformatie over de betreffende actor?	Onderhandelingen na een succesvolle ransomware aanval zal onderdeel uitmaken van de te verwerven IRR dienstverlening. Uiteraard geldt dat het bevoegd gezag in een concrete situatie op een gegeven moment daartoe een besluit dient te nemen.
46	Marktconsultatie Incident Response Retainer diensten.pdf	11	Hoofdstuk 3	Staat u open voor combinaties of onderaanneming voor specialistische onderdelen, zoals OT, mainframe, juridische ondersteuning of crisiscommunicatie? Of gaat uw voorkeur uit naar één integrale leverancier?	De Belastingdienst staat open voor combinaties en onderaanneming voor specialistische onderdelen en heeft nog geen voorkeur voor één integrale leverancier. De uitkomsten van de marktconsultatie worden betrokken bij de verwervingsstrategie. Marktpartijen kunnen in hun reactie aangeven welke inrichting zij het meest passend vinden. Eventuele voorwaarden volgen in de aanbestedingsdocumenten. Zie ook het antwoord op vraag 2.
47	Marktconsultatie Incident Response Retainer diensten.pdf	11	Hoofdstuk 3, vraag 4 en 13	Veel IR-aanbieders maken deel uit van een groep met entiteiten in meerdere EU-lidstaten. Mogen in de toekomstige opdracht medewerkers en capaciteit van groepsentiteiten in andere EU-lidstaten worden ingezet, bijvoorbeeld voor opschaling of specialistisch onderzoek? En mag een inschrijver zich voor referenties, certificeringen en geschiktheidseisen beroepen op deze groepsentiteiten?	Voor geschiktheid kan een inschrijver zich in beginsel beroepen op de capaciteiten van andere entiteiten, mits hij aantoont daadwerkelijk over de benodigde middelen te beschikken. De nadere voorwaarden worden opgenomen in de aanbestedingsdocumenten.

48			Integrale dienstverlening	Overweegt de Belastingdienst een integrale dienstverlening waarbij Incident Response, Threat Intelligence, Readiness Services en Crisismanagement binnen één retainerconstructie worden samengebracht?	Dit staat nog niet vast. Zie de algemene opmerking van de Belastingdienst.
49			MDR en Incide	Hoe ziet de Belastingdienst de samenhang tussen bestaande detectie- en monitoringdiensten (SOC/MDR) en de toekomstige Incident Response Retainer dienstverlening?	Zie het antwoord op vraag 7.
50			Preventieve in	In welke mate acht de Belastingdienst het wenselijk dat retaineruren ook kunnen worden ingezet voor preventieve activiteiten zoals readiness assessments, threat hunting, tabletop-oefeningen en verbeterprogramma's?	Belangrijk, zie vraag 40 in het marktconsultatie document. De Belastingdienst streeft naar maximale toegevoegde waarde. Zie ook het antwoord op vraag 10.
51			Cloud-prioriteit	In welke mate ziet de Belastingdienst toegevoegde waarde in proactieve dienstverlening die gericht is op het continu identificeren, prioriteren en reduceren van cyberrisico's en aanvalspaden, zodat incidenten actief kunnen worden voorkomen in plaats van uitsluitend afgehandeld?	Zie het antwoord op vraag 10.

52			Prioritering van	Welke mechanismen acht de Belastingdienst passend om beschikbaarheid en prioriteit van Incident Response-capaciteit te borgen tijdens grootschalige nationale cyberincidenten?	In het geval van nationale cyberincidenten zal de regie door een bevoegde overkoepelden overheidsinstantie worden gevoerd. De Belastingdienst gaat ervan uit dat deze regieorganisatie zich m.b.t. prioritering zal laten leiden door criteria t.a.v. vitale processen die ook ten grondslag liggen aan bijvoorbeeld de quickscan nationale veiligheid (https://www.nctv.nl/documenten/2024/02/01/quick-scan-nationale-veiligheid-bij-inkoop-en-aanbesteding).
53			CSIRT-samenv	Welke taken worden momenteel uitgevoerd door het interne CSIRT en welke activiteiten verwacht de Belastingdienst aanvullend van de toekomstige dienstverlener?	Zie het antwoord op vraag 7
54			Referentie-eise	Verwacht de Belastingdienst ervaring binnen de Rijksoverheid specifiek, of worden ook vergelijkbare organisaties binnen vitale infrastructuur, financiële dienstverlening en andere hoogbeveiligde omgevingen als relevant beschouwd?	Geschiktheidseisen zijn nog niet vastgesteld. De belastingdienst acht ervaring binnen de rijksoverheid wenselijk. Eventuele eisen worden proportioneel opgesteld en opgenomen in de aanbestedingsdocumenten.
55			Internationale e	In hoeverre acht de Belastingdienst toegang tot internationale threat intelligence en wereldwijde incidentdata van toegevoegde waarde binnen de dienstverlening?	Dit acht de Belastingdienst van evident belang. Deze informatie is een belangrijk hulpmiddel om een incident te kunnen duiden.

56			Contractvorm	Gaat de voorkeur uit naar één hoofdaannemer die integraal verantwoordelijk is voor de dienstverlening, al dan niet ondersteund door gespecialiseerde partners?	Zie het antwoord op vraag 27 en 46.
57			Maximale waar	Welke concrete diensten ziet de Belastingdienst als meest waardevol gedurende perioden waarin geen sprake is van een actief cyberincident?	Zie het antwoord vraag 10.