To: (10)(2e) [(10)(2e)@minvws.nl]
From: (10)(2e)
Sent: Tue 8/4/2020 9:27:14 AM
Subject: Fwd: RE: CIBG hosting Re: verzoek: Inkoop SOC-diensten | CoronaMelder|
Received: Tue 8/4/2020 9:27:18 AM

(10)(2e) is niet meer voor aanbesteding beschikbaar en op vakantie (10)(2e) voicemail achter gelaten.

Maar (10)(2e) lijkt toch wel lucht in het verhaal met KPN te hebben gevonden .... Dat aangrijpen en doorgaan op de dwingende spoed?

-------- Doorgestuurd bericht --------
Onderwerp: RE: CIBG hosting Re: verzoek: Inkoop SOC-diensten | CoronaMelder |
Datum: Tue, 4 Aug 2020 09:19:34 +0000
Van: (10)(2e) <(10)(2e)@rijksoverheid.nl>
Aan: (10)(2e) <(10)(2e)>

Eis 30
Hosting partij is verantwoordelijk voor de hosting van de infrastructuur en het technisch beheer van OS, middleware, databases, storage, security, webservices, netwerken en dergelijke welke gebaseerd zijn op de CIBG Enterprise Architectuur. Hosting partij voorziet in de bewaking van alle gehoste systemen, zoals websites en services. Vanuit de verantwoordelijkheid voor de operationele dienstverlening draagt hosting partij zorg voor de correcte inrichting van monitoring op systeem- en applicatieniveau. Opdrachtnemer verschaft CIBG te allen tijde toegang tot monitoring van Opdrachtnemer.

Eis 80
De infrastructuur wordt 24x7 gemonitord op zowel componentniveau als op dienst/keten niveau waarbij real time performance en beschikbaarheid zichtbaar zijn.
Deze bewaking kan voor bepaalde applicaties en websites 7x24 uur per week zijn.
Tijdens de bewaking wordt iemand gewaarschuwd bij een verstoring en er is altijd een aangewezen aanspreekpunt bereikbaar voor afnemers of medewerkers van CIBG die support kan geven.
Minimaal zal (ook) op systeemsoftware of operating systeemniveau bewaakt moeten worden.

Eis 81
Vanuit haar verantwoordelijkheid voor de operationele dienstverlening draagt de hosting partij zorg voor de correcte inrichting van monitoring op systeem- en monitoring op applicatieniveau conform de instructies van CIBG. CIBG heeft real-time inzage in de monitoring tool.

Eis 83
Indien CIBG of derde(-n) in opdracht van CIBG zelf bepaalde gegevens wil monitoren en/of auditen wordt hier volledige medewerking aan verleend.

Eis 96
De hosting partij voorziet in mogelijkheden om binnen 8 kantooruren de capaciteit uit te breiden en/of de monitoring- eisen te vergroten, zoals 7x24.

Van: (10)(2e)
Verzonden: dinsdag 4 augustus 2020 11:18
Aan: (10)(2e) <(10)(2e)>
Onderwerp: CIBG hosting Re: verzoek: Inkoop SOC-diensten | CoronaMelder |

(10)(2e),

ik weet niet exact waar de boel gehost gaat worden. Maar als het het huidige KPN BV (IS) contract met CIBG is, dan kun je hier de oorspronkelijke scope van die raamovereenkomst bekijken:
https://www.tenderned.nl/tenderned-tap/aankondigingen/110462;section=2

Zie met name de zip-file onderaan. Het document 'Beschrijvend document Managed Hosting Storage Services 20161216' beschrijft de bedoelde scope en de eisen die aan de dienstverlening zijn gesteld.

Ik zie voldoende aanknopingspunten in het PvE om te veronderstellen dat: SIEM/SOC-achtige dienstverlening al door KPN geboden wordt (cq zou moeten worden), danwel dat aanvullend een nadere offerteaanvraag kan worden gestart (onder die bestaande raamovereenkomst).
Wat stelt CIBG hierover?

Tav SIEMSOC is mijn advies om helder te verwoorden (in functionele termen) welke doelen je wilt bereiken cq welke behoeften je hebt (dat hoeft beslist geen boekwerk te zijn).
Vervolgens kan CIBG aangeven in welke mate hier al in is voorzien (zelf, door KPN danwel door derden). Op basis hiervan kunnen we bekijken welke extra (lees: nieuwe) behoeften nog resteren en hoe die het beste (rechtmatig) te verwerven.

Mvg, (10)(2e)

Van: (10)(2e)
Verzonden: maandag 3 augustus 2020 18:19
Aan: (10)(2e) <(10)(2e)>
Onderwerp: RE: VERTROUWELIJK/TLP: (10)(2e) Re: verzoek: Inkoop SOC-diensten | CoronaMelder |

Aanvullend op onderstaande.

In een eerdere aanbesteding waarbij de volgende kerncompetenties vereist zijn:
1) Continue actieve monitoring
2) Forensische capaciteit
3) Continue passieve monitoring
4) Digitale spionage door statelijke actoren

Zijn deze partijen geschikt bevonden:
- EY
- Fox-IT
- Motiv IT Masters

-----Oorspronkelijk bericht-----
Van: (10)(2e)
Verzonden: maandag 3 augustus 2020 16:37
Aan: (10)(2e) <(10)(2e)>
Onderwerp: RE: VERTROUWELIJK/TLP: (10)(2e) Re: verzoek: Inkoop SOC-diensten | CoronaMelder |

Hallo (10)(2e), bellen lijkt me verstandig.

Een dergelijk dreigingsbeeld is niet heel verrassend en zien we bij meerdere landelijke voorzieningen.

(SIEM)SOC-dienstverlening is inmiddels een tamelijke gebruikelijke behoefte die doorgaans 'normaal' wordt aanbesteedt.

Er zijn in NL verschillende partijen actief op deze markt, denk aan:
Fox IT
Deloitte Risk BV
Securelink BV
Capgemini Nederland BV
ATOS Nederland BV

Bel me zodra je in de gelegenheid bent.

Mvg, (10)(2e)

-----Oorspronkelijk bericht-----
Van: (10)(2e) <(10)(2e)>
Verzonden: maandag 3 augustus 2020 16:13
Aan: (10)(2e) <(10)(2e)@rijksoverheid.nl>
Onderwerp: VERTROUWELIJK/TLP: (10)(2e) Re: verzoek: Inkoop SOC-diensten | CoronaMelder |

Beste (10)(2e)

Onder vertrouwelijkheid (DEPV/TLP:(10)(2e)). Bijgaand is de dreigingsanalyse die we met de NCTV/AIVD/NCSC en de betrokken partijen hebben gemaakt. Duidelijk is dat er landen zijn die ons willen aanvallen (in het Oosten gelegen). Daarnaast zijn er actoren (activisten/onethische journalisten) die we verwachten zeker aan te vallen. Helpt deze informatie of moeten we anders even bellen?

Met vriendelijke groet,

(10)(2e)

Op 03-08-2020 om 16:03 schreef (10)(2e):
> Hallo (10)(2e),
>
> In beginsel geldt voor elke overheidsopdracht een aanbestedingsplicht.
>
> Uitgesloten opdrachten
> Bepaalde opdrachten worden onder de Aanbestedingswet 2012 uitgesloten van de aanbestedingsplicht.
>
> Het gaat onder meer om:
> •bepaalde opdrachten op het gebied van defensie en veiligheid;
> •opdrachten rond aanleg of exploitatie van telecom; •geheime
> opdrachten; •huur van grond en gebouwen; •aankoop van
> televisieprogramma's en zendtijd; •arbitrage en bemiddeling;
> •arbeidsovereenkomsten; •bepaalde opdrachten met betrekking tot
> onderzoek en ontwikkeling; •opdrachten op grond van een juridisch
> instrument dat internationaalrechtelijke verplichtingen schept.
> Let op: De specifieke eisen die gelden voor bovengenoemde
> uitzonderingen worden genoemd in de artikelen 2.23 tm 2.24 van de
> Aanbestedingswet 2012
>
>
> Dit wordt restrictief uitgelegd. En moeten we dus goed onderbouwen.
> Als je iets meer achtergronden van de opdracht kunt schetsten, kunnen we verkennen of 1 van deze grondslagen van toepassing is.
>
>
> Anders: onrechtmatige verwerving, opties die niet al te veel tijd vergen zijn:
> - meervoudig (tenminste 3 partijen moeten we uitnodigen)
> - rechtstreeks (technische afhankelijkheid of onverwachte dwingende
> spoed)
>
>
> Welke procedure we ook kiezen: de overheidsopdracht die we gaan gunnen moet helder zijn. Zie onderstaande vragen.
>
> Mvg, (10)(2e)
>
>
>
> -----Oorspronkelijk bericht-----
> Van: (10)(2e) <(10)(2e)>
> Verzonden: maandag 3 augustus 2020 15:43
> Aan: (10)(2e) <(10)(2e)@rijksoverheid.nl>;
> (10)(2e) (10)(2e)) <(10)(2e)@minvws.nl>
> CC: (10)(2e) <(10)(2e)@rijksoverheid.nl>
> Onderwerp: Re: verzoek: Inkoop SOC-diensten | CoronaMelder
>
> Beste (10)(2e),
>
> De vragen ga ik zo goed mogelijk proberen te beantwoorden. De vraagstelling in de richting van HIS is juist om niet onrechtmatig te zijn. Er is geen aanbestedingsplicht op het moment dat het nationale veiligheid betreft. Dat is mijn allereerste vraag. Hier is een situatie waar dit nadrukkelijk speelt. Hoe vlieg ik dat aan?
>
> Hartelijke groet,
>
> (10)(2e)
>
> (10)(2e)
>
> Op 03-08-2020 om 15:01 schreef (10)(2e):

>> Hallo (10)(2e),
>>
>> Kun jij onderstaande behoefte nader duiden cq een HIS inkoopaanvraag opstarten svp?
>>
>> Van belang is:
>> - duidelijke behoeftestelling (exact welke diensten en servicelevels
>> hebben we minimaal nodig?) incl afhankelijkheden (context informatie,
>> welke systemen, welk DC, welke hostingpartij etc.)
>> - wie is aanspreekpunt voor deze aanbesteding
>> (projectleider/coördinator die vervolgens de materiedeskundigen
>> alloceert)
>> - inventarisatie inbesteden (RWS, Defensie, BD, Logius hebben
>> soortgelijke diensten)
>> - inventarisatie evt. bestaande raamovereenkomsten VWS
>> - gewenste ingangsdatum, minimale looptijd van de overeenkomst
>> - verwachte optionele diensten (= toekomstige uitbreidingen van de
>> opdracht)
>> - raming van de opdrachtwaarde
>> - mogelijke partijen die deze opdracht kunnen uitvoeren (tenminste 3
>> tbv een meervoudige procedure) ofwel een deugdelijke motivering
>> waarom er maar 1 partij is die dit kan uitvoeren (tbv
>> rechtstreeksgunnen) incl contactgegevens
>> - indien noodzakelijk: akkoord tbv onrechtmatigheid vanuit (10)(2e)
>>
>> Dankjewel alvast,
>>
>> Met vriendelijke groet,
>>
>> (10)(2e)
>> (10)(2e)
>> .....
>> UBR|HIS
>> Uitvoeringsorganisatie Bedrijfsvoering Rijk Ministerie van
>> Binnenlandse Zaken en Koninkrijksrelaties Beatrixpark, Wilhelmina van
>> Pruisenweg 52 | 2595 AN | Den Haag Postbus 20011 | 2500 EA | Den Haag
>> .....
>> M (10)(2e)
>> (10)(2e) @rijksoverheid.nl
>> www.UBRijk.nl/HIS
>>
>> -----Oorspronkelijk bericht-----
>> Van: (10)(2e)) < (10)(2e) @minvws.nl>
>> Verzonden: maandag 3 augustus 2020 14:55
>> Aan: (10)(2e) < (10)(2e) >; (10)(2e)
>> < (10)(2e) @rijksoverheid.nl>
>> CC: (10)(2e) < (10)(2e) @dictu.nl>; (10)(2e)
>> < (10)(2e) @ctinterim.nl>
>> Onderwerp: RE: Inkoop SOC-diensten
>>
>> Zeker en bij deze, we hebben deze SOC-diensten hard nodig én acuut !
>>
>> Met groet,
>>
>>
>> (10)(2e) (10)(2e) | (10)(2e)
>> (10)(2e) | Directie Informatiebeleid| Ministerie van
>> Volksgezondheid, Welzijn en Sport | Parnassusplein 5 | 2511 VX | Den
>> Haag | Postbus 20350 | 2500 EJ | Den Haag | ☐ | (10)(2e) |(10)(2e)
>> (10)(2e) |(10)(2e)| (10)(2e) (10)(2e)
>> (10)(2e) @minvws.nl | www.rijksoverheid.nl |
>>
>>
>>
>>
>> -----Oorspronkelijk bericht-----
>> Van: (10)(2e) < (10)(2e) >
>> Verzonden: maandag 3 augustus 2020 12:15
>> Aan: (10)(2e) < (10)(2e) @rijksoverheid.nl>
>> CC: (10)(2e)) < (10)(2e) @minvws.nl>; (10)(2e)
>> < (10)(2e) @dictu.nl>; (10)(2e) < (10)(2e) @ctinterim.nl>
>> Onderwerp: Inkoop SOC-diensten

>>
>> @(10)(2e): kun jij svp naar (10)(2e) bevestigen dat wij SOC-diensten nodig hebben.
>>
>> Beste (10)(2e),
>>
>> Dank voor je bericht via (10)(2e) met betrekking tot de bewaking van CoronaMelder.
>>
>> Graag leg ik een en ander goed uit.
>>
>> Korte termijn
>>
>> Ik las ook je opmerking over de korte termijn. Dat leg ik graag uit. Wij konden gebruik maken van het Security Operations Center van de Belastingdienst. Alleen toen de Staatssecretaris van Financien besloot dat CoronaMelder geen gebruik meer mocht maken van diensten van de Belastingdienst viel deze ondersteuning ook weg. Pas wanneer je weet waar de serverkant terecht komt en hoe dat eruit kan zien, kun je hosting regelen. De dwingende spoed is niet onze keuze zeg maar.
>>
>> CoronaMelder en Nationale Veiligheid
>>
>> CoronaMelder is een app die beoogt mensen eerder te waarschuwen voor een verhoogde kans op besmetting met het Corona-virus. Door eerder te zijn, wordt de verspreiding van het virus geremd. Logischerwijs zullen minder mensen langdurige ziekten als COPD of hartfalen contracteren. Het kan de kwaliteit van leven verhogen en forse economische schade remmen.
>>
>> Echter hebben we in samenwerking met de NCTV en de AIVD vastgesteld dat er actoren zijn die dit proces zullen proberen te verstoren. Met oog op een aantal van deze risico's speelt ook een staatsgeheim. In de verdediging is bewaking nodig. Dat regel je normaliter via een security operations center. Gelet op de gevoeligheid en de complexiteit heb je daarvoor dan gespecialiseerd SOC nodig. Daarvoor kijken wij naar KPN 'KDNV' (KPN Defensie en Nationale Veiligheid).
>>
>> Nogmaals: dat we op een tijdkritisch pad zitten is echt situationeel gedreven en absoluut niet onze wens geweest. Gelet op het gevoelige karakter kan ik echt de hulp gebruiken hoe we dit correct en rechtmatig gaan inregelen.
>>
>> Hartelijke groet,
>>
>> (10)(2e)
>>
>> (10)(2e)
>>