Tweede Nota van Inlichtingen

Europese openbare aanbestedingsprocedure
‘Ondersteuning ICT kantoorautomatisering’

Datum: 19-01-2026

Deze tweede Nota van Inlichtingen is opgebouwd uit drie delen: DEEL A, DEEL B en DEEL C.

Onderstaand overzicht van de mededelingen (DEEL A), van de wijzigingen (DEEL B) en van de gestelde vragen met de daarbij behorende antwoorden (DEEL C) dient te worden beschouwd als een integraal onderdeel van de Aanbestedingsleidraad ‘Ondersteuning ICT kantoorautomatisering’ van 26 november 2025.

De gestelde vragen zoals opgenomen in deze tweede Nota van Inlichtingen zijn letterlijk (met uitzondering van eventuele bedrijfsnamen van vragen stellende partijen, deze zijn vervangen door ‘leverancier’) overgenomen zoals deze zijn gesteld.

DEEL A. Betreffende de mededelingen

Nr.	Verwijzing	Mededeling
1	Aanbestedings-leidraad, paragraaf 1.5 en 3.3	In verband met het wijzigen van de geschiktheidseisen wordt de planning van de aanbestedingsprocedure aangepast en wordt een derde inlichtingenronde ingelast. Zie DEEL B nummer 1 en 2 van deze tweede Nota van Inlichtingen.

DEEL B. Betreffende de wijzigingen

Nr.	Verwijzing	Wijziging
1	Aanbestedings-leidraad 4.3.2.2	Geschiktheidseis 2 ‘SOC2 Type I of een ISAE 3402 Type I verklaring’ komt in zijn geheel te vervallen.
2	Programma van Eisen, eis 30	Eis 30 komt in zijn geheel te vervallen.
3	Aanbestedings-leidraad, Checklist voor het indienen van een inschrijving, pag. 2	Het, als verplicht onderdeel van de inschrijving, indienen van een bewijsstuk beschikken over geldige SOC2 Type I of een ISAE 3402 Type I verklaring komt te vervallen.
4	Aanbestedings-leidraad, paragraaf 1.5	De planning van de aanbestedingsprocedure wordt gewijzigd conform onderstaande tabel. De wijzigingen zijn groen gemarkeerd. De gebeurtenissen die reeds zijn afgerond of die ongewijzigd blijven zijn geel gemarkeerd.

Activiteit	Datum	Tijd (CET)
Publicatie	26-11-2025	
Uiterste datum voor het stellen van vragen, eerste inlichtingenronde	08-12-2025	10:00u
Publicatie eerste Nota van Inlichtingen	Beoogd uiterlijk op 15-12-2025	
Uiterste datum voor het stellen van vragen, tweede inlichtingenronde	12-01-2026	10:00u
Publicatie tweede Nota van Inlichtingen	Beoogd uiterlijk op 19-01-2026	
Uiterste datum voor het stellen van vragen, derde inlichtingenronde	26-01-2026	
Publicatie derde Nota van Inlichtingen	Beoogd uiterlijk op 30-01-2026	
Sluitingstermijn voor het indienen van een inschrijving	**10-02-2026**	**12:00u**
Openen inschrijvingen en start beoordeling	Vanaf 10-02-2026	

Nr.	Verwijzing	Wijziging
		<table><tr><td>Toelichtingsgesprekken</td><td>Beoogd op 18-02-2026</td></tr><tr><td>Verzenden gunningsbeslissing, start bezwaartermijn en verificatiefase</td><td>Beoogd op 03-02-2026</td></tr><tr><td>Ondertekenen overeenkomst</td><td>Beoogd vanaf 23-03-2026</td></tr><tr><td>Ingangsdatum overeenkomst en start niet-operationele implementatieperiode</td><td>Beoogd op 01-04-2026</td></tr><tr><td>Einde niet-operationele implementatieperiode</td><td>Beoogd op 30-06-2026</td></tr><tr><td>Start operationele dienstverlening</td><td>Beoogd op 01-07-2026</td></tr></table>
5	Aanbestedings-leidraad, 5.2.4	**LET OP:** de datum waarop de toelichtingsgesprekken plaatsvinden is gewijzigd naar **18-02-2026**. De definitieve uitnodiging voor het toelichtingsgesprek inclusief de locatie en het tijdstip volgt zo spoedig mogelijk na de sluitingsdatum voor het indienen van de inschrijving. De inschrijver wordt verzocht de datum van 18-02-2026 op voorhand vrij te houden in de agenda’s van de betrokken personen.
6	Aanbestedings-leidraad, 2.5 lid A Beheer en ondersteuning	Op basis van nieuw verkregen inzichten is besloten het volledige beheer van de firewall uit te besteden aan een externe partij. Als gevolg hiervan maakt het beheer van de firewall **géén** onderdeel meer uit van de scope van deze aanbesteding.

DEEL C. Betreffende de gestelde vragen

Nr.	Verwijzing	Vraag	Antwoord
1	Par. 4.3.2.2, p. 24	U vereist een SOC2 en/of ISAE 4302-verklaring. Hierbij geeft u tevens aan dat bij een samenwerkingsverband de penvoerder over deze verklaring moet beschikken. Wij wijzen u erop dat dit geen gangbare verklaringen zijn van een opdracht van deze aard en omvang. Deze verklaringen zijn met name relevant voor opdrachten met een grootschalige hosting- of outsourcingcomponent en/of grote hoeveelheden financiële/vertrouwelijke dataverwerking (denk aan hosting/beheer van ERP-systemen of uitbesteding financiële administratie). Dergelijke certificaten wrorden dan ook vrijwel uitsluitend gevoerd door grote datacenterpartijen, cloud providers en de echt grote MSP’s die ook veel aan enterprise outsourcing doen. Niet het soort MSP’s dat als hoofdinschrijver deelneemt aan aanbestedingen als deze. Het uitvragen van deze verklaring is derhalve disproportioneel en hiermee beperkt u de mededinging onnodig. Inschrijver verzoekt daarom deze eis te laten vervallen; of indien u hier niet mee akkoord bent, de eis aan te passen zodat niet per definitie de penvoerder of hoofdinschrijver, maar de partij die de hosting van de servers verzorgt dient te beschikken over deze verklaring.	Het Commissariaat wordt jaarlijks door externe accountants onderworpen aan een ICT-audit. Op basis van dit accountantsonderzoek wordt aanbevolen om bij aanbestedingen te verzoeken om een SOC2- en/of ISAE4302-verklaring. Wij erkennen echter, in lijn met de inschrijver, dat deze eis mogelijk niet proportioneel is gezien de omvang van zowel de organisatie als de opdracht. Daarom is besloten deze eis te laten vervallen. Zie ook DEEL B nummer 1 van deze tweede Nota van Inlichtingen.

Nr.	Verwijzing	Vraag	Antwoord
2	Par. 4.3.2.2, p. 24	In het geval u vasthoudt aan SOC2 /ISAE voor de partij die de servers host: Hier vraagt u een SOC Type I of ISAE 3402 Type I; in het programma van eisen een SOC 2 Type II of ISAE Type II. Welke is juist? In de praktijk wordt Type II geaccepteerd als vervanging van Type I; omdat Type II alle elementen bevat van een Type I en daarnaast de werking van de maatregelen over een langere periode aantoont. Gaat u hiermee akkoord?	Zie het antwoord op vraag 1; de eis voor een SOC2 / ISAE4302 certificering komt te vervallen.
3	Par. 4.3.2.2, p. 24	Inschrijver beschikt nog niet over een ISO 9001 certificering, maar wel over gelijkwaardige maatregelen op het gebied van kwaliteitsmanagement en wij zitten in een traject voor certificering. Inschrijver wijst erop dat conform art. 2.96 Aw2012 bij het vereisen van certificeringen als geschiktheidseis ook vergelijkbare certificaten of andere bewijzen inzake gelijkwaardige maatregelen dienen te worden geaccepteerd, als kan worden aangetoond dat het certificaat om redenen die hem niet kunnen worden aangerekend niet tijdig kon worden verkregen. Wij verzoeken u derhalve toe te staan dat deze eis kan worden aangetoond d.m.v. een beschrijving van de getroffen maatregelen en onderbouwing van gelijkwaardigheid, al dan niet vergezeld door een planning van de certificering. Gaat u hiermee akkoord? Zo nee, graag uw toelichting waarom niet, gelet op voornoemde bepaling uit de Aanbestedingswet.	Inschrijver dient over een ISO 9001 certificering of een gelijkwaardig systeem voor kwaliteitsborging te beschikken. Indien inschrijver een gelijkwaardig alternatief voor ISO 9001 certificering gebruikt dan dient hij de gelijkwaardigheid aan te tonen door middel van het indienen van een beschrijving van het kwaliteitsmanagementsysteem dat getoetst is door een externe audit partij.
4	Bijlage II	U geeft een overzicht van licenties, maar zonder aantallen. Deze informatie is nodig om ons een goed beeld te vormen van de omvang en scope van de opdracht. Wij verzoeken u om deze informatie te verstrekken.	Zie ‘Bijlage NvI 1.xlsx’, tabblad ‘Licentieoverzicht’.

Europese openbare aanbestedingsprocedure ‘Ondersteuning ICT kantoorautomatisering’

Nr.	Verwijzing	Vraag	Antwoord
5	Bijlage 11	In bijlage 4 (prijzenblad) verwijst u naar bijlage 11 voor de licenties. Kunt u aangeven hoeveel van iedere licentie moet worden opgenomen voor de prijs in het prijzenblad?	Zie het antwoord op vraag 4.
6	Aanbestedings-leidraad	Is de bestaande Sophos XGS 2300 enkelvoudig of redundant uitgevoerd?	In de aanbesteding is er aangegeven dat het beheer van de firewall onderdeel is van de opdracht. Dit is echter niet het geval, de firewall zal door een derde partij worden beheerd. Zie ook DEEL B nummer 6 van deze tweede Nota van Inlichtingen.
7	Aanbestedings-leidraad	Wanneer verloopt de huidige enhanced support licentie van de de Sophos XGS 2300?	Zie het antwoord op vraag 6.
8	Bijlage 5 PvE	Punt 10, wat is de gewenste retentie voor het bewaren van de backup?	1 jaar.
9	Algemeen	Kunt u een overzicht delen met hier in de volgende gegevens: - Aantal actief gebruikers, uitsplitst in rollen als Kenniswerker, heavy user, task work etc. - Aanwezig laptops, vaste plekken met type, merk , aanschafdatum, besturingssysteem. - Overzicht servers, OS versie. - Switches, Access points - Overige apparatuur binnen scope van de beheeropdracht	Binnen het Commissariaat is geen onderscheid in type gebruiker, enkel onderscheid tussen interne en externe medewerker. Dit maakt weinig verschil. Van de externe medewerkers gaan wij in het beginsel er vanuit dat zij hun eigen apparatuur gebruiken, hierdoor krijgen zij enkel een ‘online-only’ licentie (zoals Microsoft 365 Business Basic), tenzij anders wordt afgesproken. Voor een overzicht van de aanwezige laptops en aanschafdatum, zie ‘Bijlage Nvl 1.xlsx’, tabblad ‘Aanwezige laptops’. Alle laptops zijn voorzien van Windows 11. Er zijn geen vaste werkplekken met bijvoorbeeld desktops die beheerd worden. Er zijn 2 Microsoft Server’s in onze Azure tenant, deze hebben zijn beide Windows Server 2019 (1809). Switches en access points vallen buiten de opdracht. Ook is er geen overige apparatuur dat binnen de beheeropdracht valt.
10	Aanbestedings-leidraad	Pagina 32, onder het kopje "Implementatie", "Aanpassen van de bestaande omgeving naar nieuwe baselines." Naar welke nieuwe baselines verwijst u hier?	In de huidige situatie wordt de bestaande omgeving beheerd door een externe partij. Deze partij heeft een eigen baseline opgesteld waarin staat beschreven aan welke (beveiliging)eisen de ICT-omgeving dient te voldoen. Door middel van dit punt willen wij de inschrijver de mogelijkheid geven om de inrichting te laten voldoen aan de richtlijnen die de opdrachtnemer als adequaat acht.
11	Aanbestedings-leidraad	Pagina 32, kunt u aangeven op welke punten de huidige omgeving niet voldoet aan de nieuwe gewenste baseline?	Zie het antwoord op vraag 10.

Nr.	Verwijzing	Vraag	Antwoord
12	Leidraad hoofdstuk 2.5	U vraagt onder k) Het beheren en monitoren van de huidige SIEM oplossing (XDR/Microsoft Sentinel) en acteren op meldingen. Is dit gedurende 24x7?	Nee, dit is gedurende kantooruren.
13	Leidraad §2.5, §2.6 | PvE algemeen	Wat is het exacte aantal medewerkers, gebruikersaccounts in de Microsoft 365 / Azure tenant en het aantal werkplekken/devices dat binnen de scope van deze opdracht valt, ten behoeve van correcte inschatting van de omvang van beheer-, support- en SIEM-dienstverlening?	Op dit moment zijn er 107 medewerkers gebruikersaccounts, waarvan 96 van interne medewerkers zijn. De overige zijn externe medewerkers/inhuurkrachten/ZZP’ers. Daarnaast zijn er 35 accounts die als gedeelde mailbox dienen, 10 serviceaccounts, 4 test accounts. Er zijn 2 Microsoftservers die binnen het beheer vallen, en iedere medewerker, zowel intern als extern, valt binnen de scope van beheer (zie ook het antwoord op vraag 9).
14	Leidraad §2.5 A(b)(g) | PvE art. 8, 18–24	Welke typen werkplekken zijn in gebruik (Windows/macOS)?	Alle apparatuur dat wij uitleveren is Windows. Telefoons zijn wel iOS.
15	Leidraad §2.5 A(b)(g) | PvE art. 8, 18–24	Wordt Intune ingezet voor device management? Zo ja met welke beleidsinrichting, mede gezien de impact op complexiteit en beheerinspanning?	Apparaten worden toegevoegd aan de Intune / AutoPilot omgeving. Apparaten dienen *compliant* te zijn voordat zij via de laptopomgeving toegang kunnen krijgen tot de bedrijfsbronnen. De beleidsregels die hiervoor gelden zijn te vinden in ‘Bijlage Nvl 1.xlsx’, tabblad ‘Device Compliance’. Vanuit Intune worden ook bepaalde kantoorapplicaties en configuraties toegepast op de apparaten.
16	Leidraad §2.5 A(c)(k) | PvE art. 8	Is Azure-beheer expliciet onderdeel van de scope? Zo ja, welke Azure-resources en subscriptions vallen hieronder, gezien de directe impact hiervan op scope en prijsstelling?	Azure-beheer is een breed begrip gezien Azure uit honderden producten bestaat. In het beginsel gaat het beheer hier om Azure producten die nodig zijn voor de kantoorautomatisering, zoals bijvoorbeeld Entra, Intune, Exchange, etc. Het inrichten van Azure-resources zal in principe bij de eigen systeembeheerder komen te liggen. Maar indien dit voor de systeembeheerder niet haalbaar is (bijvoorbeeld i.v.m. andere prioriteiten, afwezigheid of ontbrekende kennis), kan dit bij de opdrachtnemer worden belegd op opdrachtbasis. Het ‘na beheer’ hangt af van de resource. Een lijst van de huidige resources is te vinden in ‘Bijlage Nvl 1.xlsx’, tabblad ‘Azure Resources’.

Nr.	Verwijzing	Vraag	Antwoord
17	Leidraad §2.5 A(k) | PvE art. 25	Kunt u de huidige en gewenste scope van de SIEM-oplossing (XDR / Microsoft Sentinel) specificeren inclusief aangesloten databronnen, indicatief logvolume, gewenste responstijden en inzetvensters, aangezien dit substantiële impact heeft op prijs en capaciteit?	Onze huidige SIEM oplossing is Microsoft Sentinel. De volgende data connectors zijn actief: Azure Activity, Microsoft 365, onder Microsoft Defender: for Endpoint, for Identity, for Office 365, Threat Intelligence, XDR, for Cloud Apps en Microsoft Entra ID. De logs en alerts van de databronnen komen binnen op de Log Analytics workspace. De retentieperiode is 90 dagen. Het monitoren, analyseren en afhandelen gebeurt via Azure Lighthouse. Ad-hoc wordt toelichting gegeven op SIEM-gerelateerde vragen ten behoeve van analyses of incidenten. Maandelijks wordt een rapport opgesteld waarin weer wordt gegeven welke dreigingen/incidenten plaats hebben gevonden en welke prioriteit deze hadden. In de huidige opstelling wordt er binnen 30 minuten een triage uitgevoerd en wordt de urgentie bepaald. Bij een hoge urgentie wordt er verder onderzoek binnen 30 minuten uitgevoerd, medium 2 uur en low 4 uur. Bij Medium/High incidenten er met de eindgebruiker (indien van toepassing) contact opgenomen en met de contactpersoon van het Commissariaat. Indien noodzakelijk gebeurt dit ook bij Low incidenten. Incidenten dienen ook geregistreerd te worden. Dit gebeurt allemaal onder kantoortijden. Met deze manier van werken is het Commissariaat tevreden en heeft op dit moment geen verbeteringen of wijzigingen voor ogen.
18	Leidraad §2.5 A(j)(k) | PvE art. 13, 22, 25	Welke Microsoft 365 / Azure security-functionaliteiten zijn actief en vallen onder beheer en monitoring (zoals Defender, Conditional Access, DLP, Access Packages en MFA) om de vereiste security-inzet correct te kunnen bepalen?	We maken gebruik Conditional Access. De voornaamste regels hierin zijn het vereisen van MFA (TOTP of Microsoft Authenticator), toestaan/blokkeren van landen. Daaronder valt ook nog Named Locations, waarin verschillende blokkades of toegang is ingeregeld voor specifieke IP’s of landen. Van Access Packages en Data Loss Prevention binnen Purview (DLP) wordt momenteel geen gebruik gemaakt. De monitoring van bijvoorbeeld meervoudige

Nr.	Verwijzing	Vraag	Antwoord
			geblokkeerde inlog pogingen zal in het SIEM opgenomen dienen te worden.
19	Leidraad §2.5 A(h)(k)	Wat is de huidige Microsoft Secure Score (4stuks) en wordt van de opdrachtnemer verwacht dat deze actief wordt verhoogd en periodiek wordt gerapporteerd, ter bepaling van de security-volwassenheid en verbeterinspanning?	Identity: 66,30% Data: 22,20% Device: 81,82% Apps: 93,08% (Secure Score: 82,41%, organisations of a similar size: 43,65%) Het Commissariaat vindt een goede inspanning voor beveiliging/security belangrijk. Wij gaan er wel van uit dat hier periodiek, bijvoorbeeld eens per half jaar, wel naar wordt gekeken om te kijken waar gemakkelijk punten gescoord kunnen worden – het lijkt ons onlogisch hier nimmer naar te kijken. Een periodiek (gedetailleerd) rapport is geen vereiste.
20	PvE art. 20–21	Kan inschrijver ervan uitgaan dat de supporttijden (08:00–18:00) ook van toepassing zijn op security- en SIEM-incidenten? Zo nee, graag uw toelichting.	Ja, dat is correct.
21	Leidraad §2.5 A(k) | PvE art. 25	Hoe is de rol- en verantwoordelijkheidsverdeling bij security-incidenten tussen opdrachtgever en opdrachtnemer ingericht? Dit om interpretatieverschillen tijdens uitvoering te voorkomen.	Indien er vanuit monitoring security-incidenten worden geconstateerd, dan dienen deze onverwijld doorgegeven te worden aan de interne systeembeheerder die actie zal ondernemen. Indien de opdrachtnemer vanuit zijn expertise een beveiligingsprobleem als zeer urgent classificeert heeft de opdrachtgever het mandaat om zonder overleg mitigerende maatregelen te treffen.
22	Leidraad §2.6	Zijn er verwachte uitbreidingen in gebruikers, devices, Azure-resources of security-functionaliteit gedurende de looptijd van de overeenkomst die relevant zijn voor schaalbaarheid en prijsstelling?	Ja, naar verwachting zullen er nieuwe medewerkers starten in 2026 waardoor ook het aantal licenties zal oplopen. Daarnaast is het CvdM bezig met het opzetten van een Datalake (Databrix) in Azure. De exacte inrichting van het datalake is op moment van schrijven nog niet duidelijk.
23	PvE art. 18–20 | Leidraad §2.5	Kunt u bevestigen dat het ITSM-systeem van de opdrachtgever leidend is voor alle ticketregistratie en -afhandeling, waarbij incidenten en verzoeken altijd via dit systeem worden ingediend en de opdrachtnemer uitsluitend 2e en 3e-lijnsondersteuning levert in afstemming met de interne systeembeheerder van de opdrachtgever? Tevens ontvangen wij graag bevestiging dat deze werkwijze ongewijzigd blijft bij afwezigheid van de interne systeembeheerder, zodat voor	Dit is inderdaad het uitgangspunt, maar indien er de voorkeur wordt gegeven aan het gebruik van het ITSM systeem van de opdrachtnemer dan is dat bespreekbaar. In de praktijk zullen alle vragen en incidenten binnenkomen in de ITSM tool van het Commissariaat. Indien de vraag of incident geëscaleerd wordt naar de opdrachtnemer, dan is het weinig moeite om een ticket aan te maken in het systeem van de opdrachtnemer. Deze werkwijze blijft ongewijzigd bij afwezigheid van de interne systeembeheerder.

Nr.	Verwijzing	Vraag	Antwoord
		eindgebruikers geen alternatieve meldroute of werkwijze ontstaat.	
24	PvE art. 8, 15, 16 | Leidraad §2.5	Kunt u specificeren welke serverplatformen onderdeel zijn van de scope van deze aanbesteding (bijvoorbeeld on-premises servers, virtualisatieplatformen zoals VMware en/of Azure-gebaseerde servers), inclusief per platform het type (fysiek/virtueel), merk en model, leeftijd, resterende garantie- en supportstatus en eventuele lifecycle-afspraken?	Er zijn 2 virtuele Microsoft Server’s in onze Azure tenant, deze hebben zijn beide Windows Server 2019 (1809). Van on-premises wordt momenteel geen gebruik gemaakt, dus zijn er geen afspraken m.b.t. garanties en lifecycles.
25	PvE art. 8, 19, 22, 24 | Leidraad §2.5	Kunt u verduidelijken welke tooling momenteel wordt gebruikt voor server- en werkplekbeheer, in het bijzonder voor patching, monitoring en remote access, en bevestigen of de opdrachtnemer bevoegd is om hiervoor eigen standaard tooling uit te rollen en te beheren? Indien bestaande tooling verplicht is, ontvangen wij graag een specificatie hiervan en de daarbij behorende verantwoordelijkheidsverdeling.	Momenteel wordt er gebruikt gemaakt van Datto RMM om werkplekken vanaf afstand te beheren. Dit draait ook op beide servers, al wordt doorgaans Microsoft Remote Desktop gebruikt hiervoor. Updates (patching) verlopen gewoon via Windows Updates, hiervoor is geen speciale tooling. De opdrachtnemer is bevoegd over te gaan naar een softwarepakket/tooling die hen voorkeur heeft en dit geen meerkosten met zich meebrengt. Het gebruik of overname van Datto RMM is niet verplicht.
26	PvE art. 10–11 | Leidraad §2.5	Kunt u specificeren welke systemen en data onder de back-upoplossing vallen (waaronder servers, Microsoft 365 en eventuele Azure-resources), inclusief een indicatie van het huidige datavolume per component, de verwachte jaarlijkse groei, de gewenste retentieperioden en of herstelwerkzaamheden zoals restore-tests en calamiteitenherstel onderdeel zijn van de scope van de opdrachtnemer?	Zie bijlage ‘Bijlage NvI 2.docx’, hierin wordt beschreven hoe de huidige backups zijn ingeregeld. Hier is het Commissariaat tevreden mee en heeft geen wijzigingen of verbeteringen voor ogen. Het installeren, configureren en beheren van een backup is voor de opdrachtnemer. Controles en 1e lijns probleemoplossing m.b.t de backups dient door de interne systeembeheerder uitgevoerd te kunnen worden.
27	PvE art. 22–23	Wordt van de opdrachtnemer verwacht dat bij monitoringmeldingen proactief herstelacties worden uitgevoerd, of uitsluitend dat signalering plaatsvindt en afstemming met de interne systeembeheerder vereist is alvorens actie wordt ondernomen?	Bij monitoringsmeldingen dient er met de interne systeembeheerder te worden afgestemd, tenzij het de inschatting van de opdrachtnemer is dat een incident dermate kritiek is dat onmiddellijk handelen genoodzaakt is.
28	PvE art. 8, 22	Zijn er vastgestelde onderhouds- en patchwindows voor servers en werkplekken en gelden hiervoor specifieke goedkeurings-, communicatie- of escalatieprocedures richting de opdrachtgever?	Werkzaamheden waardoor er systemen tijdelijk niet werken dienen na 18.00u of in het weekend te worden uitgevoerd. Voor periodiek onderhoud is hier geen speciale procedure voor op gesteld anders dan het tijdig melden van de voorziene downtime.
29	Leidraad §2.5, p.7	Er zijn twee vragenrondes voorzien, waarvan de eerste vrij snel na publicatie. Hier zijn geen vragen ontvangen. Wij – en wellicht andere marktpartijen – hebben wel vrij vlot daarna vragen ingediend, maar deze	De planning van de aanbestedingsprocedure is aangepast. Zie ook DEEL B nummer 4 van deze Nota van Inlichtingen.

Nr.	Verwijzing	Vraag	Antwoord
		worden pas beantwoord bij de tweede nota van inlichtingen. De tweede nota staat gepland voor uiterlijk 19 januari. Hierna zijn er nog precies 2 weken (in de praktijk 9 werkdagen) tot de inschrijftermijn. Deze termijn is erg kort om een kwalitatieve aanbieding te kunnen doen. Daarnaast is redelijkerwijs te verwachten dat er nog vervolgvragen komen, gelet op de aard van onze vragen en wat gebruikelijk is bij aanbestedingen voor kantoorautomatisering. Het feit dat er in de eerste vragenronde geen vragen zijn gesteld is ons inziens geen teken dat die er niet zijn, maar dat ofwel deze ten tijde van de eerste Nota nog niet helder waren, ofwel er weinig inschrijvers zijn. Hoe dan ook is het in het belang van alle betrokkenen, van de kwaliteit van de inschrijving en het slagen van de aanbesteding, dat inschrijvers voldoende gelegenheid hebben om de opdracht te doorgronden en een goede, passende inschrijving te kunnen doen. Wij verzoeken u daarom de inschrijftermijn te verlengen met 3 weken en daarnaast een extra vragenronde in te stellen. Gaat u akkoord met ons voorstel? Zo nee, graag uw toelichting.	