Uitvoeringsorganisatie
Bedrijfsvoering Rijk
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Inkoop
Nota van Inlichtingen

UBR|HIS

Bezoekadres
Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

GEGEVENS AANBESTEDING	
Kenmerk	201850004.160.002
Betreft Dynamisch aankoopsysteem	Security & penetratietesten
Datum	29 juli 2025

Dit is de Nota van Inlichtingen waarin de gestelde vragen van de Potentiële Aanmelders, naar aanleiding van het Toelatingsleidraad 1.5, worden beantwoord.

TOELATINGSLEIDRAAD

Algemeen:
De vragen die hieronder gesteld worden zijn allemaal zeer relevant, maar zullen doorgaans geadresseerd worden in losse offerte uitvragen onder deze DAS. Die zullen verschillen per voorziening of platform. Logius dicteert dit niet top down.

VRAAG 1	Welke specifieke leveringen worden er verwacht van elk type test (bijvoorbeeld black box, grey box, white box, red teaming)?
Vindplaats	Penetratie testen
Antwoord	Je hoeft geen ART of TIBER test te kunnen aanbieden, maar deze kan wel uitgevraagd worden. DigiD assessments worden ook uitgevraagd onder de DAS.

VRAAG 2	Zijn er specifieke systemen, platforms of technologieën (bijvoorbeeld cloud services, IoT, legacy systemen) binnen de huidige scope van testen?
Vindplaats	Penetratie testen
Antwoord	Nee, hier worden geen eisen aan gesteld. Systemen, platformen en technologieën in gebruik zijn er te veel om hier op te sommen. Dit wordt geadresseerd in een specifieke uitvraag onder de DAS.

VRAAG 3	Is er een voorkeurs- of verplichte testmethodologie of standaard (bijvoorbeeld OWASP, OSSTMM, NIST)?
Vindplaats	Penetratie testen
Antwoord	In de toelatingsleidraad zijn hier geen eisen aan gesteld. Doorgaans wordt gevraagd te testen tegen de OWASP top tien CWE/SANS top 25. Dat is echter geen methodiek. Bij een offerteaanvraag kun je mogelijk meer punten verdienen met een gestandaardiseerde testmethodologie.

VRAAG 4	Wat zijn de beveiligings- en wettelijke vereisten rond exploitatie, mogen testers potentieel verstorende payloads uitvoeren (bijvoorbeeld privilege escalation, data exfiltration) tijdens white box of red teaming oefeningen?
Vindplaats	Penetratie testen
Antwoord	Dit kan verschillen per opdracht/uitvraag en kan per opdracht afspraken over worden gemaakt.

VRAAG 5	Zijn er specifieke rapportage- of communicatieprotocollen tijdens de testfase (bijvoorbeeld tussentijdse updates, incident notificatieprocedures)?
Vindplaats	Penetratie testen
Antwoord	Hier zijn geen eisen aan gesteld in de Toelatingsleidraad. Conform gebruikte methodologie en onderlinge afspraken.

VRAAG 6	Wat zijn de doelstellingen en succescriteria van de test (bijvoorbeeld het identificeren van kwetsbaarheden, testen van incidentrespons, demonstreren van laterale beweging)?
Vindplaats	Penetratie testen
Antwoord	Doorgaans wordt gevraagd te testen tegen de OWASP top tien CWE/SANS top 25.

VRAAG 7	Zijn er beperkingen met betrekking tot testtijd, werkuren of juridische/contractuele naleving (bijvoorbeeld vereiste meldingen, land specifieke wetten)?
Vindplaats	Penetratie testen
Antwoord	Alleen als deze in de uitvraag staan.

VRAAG 8	Zijn er kritieke systemen of omgevingen (bijvoorbeeld productiedatabases, gezondheidszorgsystemen) waar testen beperkt of uitgesloten moeten worden om verstoring te voorkomen?

Vindplaats	Penetratie testen
Antwoord	Dit zal worden aangegeven in individuele uitvragen.

VRAAG 9	Welk niveau van toegang of informatie zal worden verstrekt in elk type penetratietest?
Vindplaats	Penetratie testen
Antwoord	Dat zal verschillen afhankelijk van bijvoorbeeld een blackbox of crystal box pentest. Dit zal worden aangegeven in individuele uitvragen.

VRAAG 10	Zal er een contactpunt of incidentrespons team beschikbaar zijn tijdens het testen in geval van kritieke bevindingen of onbedoelde impact?
Vindplaats	Penetratie testen
Antwoord	Ja

VRAAG 11	Zijn er specifieke compliance- of regelgevingsvereisten (bijvoorbeeld GDPR, ISO 27001, PCI-DSS) waarmee de testen moeten voldoen of waar ze op moeten aansluiten?
Vindplaats	Penetratie testen
Antwoord	Nee, tenzij aangeven in een specifieke uitvraag.

VRAAG 12	Wat zijn de doelstellingen van de phishingcampagne (bijvoorbeeld het beoordelen van gebruikersbewustzijn)?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Verhogen van I-Bewustzijn en digitale weerbaarheid van Logianen.

VRAAG 13	Wie is de doelgroep voor de campagne (bijvoorbeeld alle medewerkers, specifieke afdelingen, het management)?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Dit kan verschillen per opdracht.

VRAAG 14	Wat voor soort phishingmethoden moeten worden gebruikt (bijvoorbeeld e-mail, SMS, voice phishing)?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Alle bovengenoemde methodieken zijn in het verleden gebruikt.

VRAAG 15	Wat zijn de acceptabele thema's (bijvoorbeeld interne HR-berichten, valse facturen, pakketlevering)? Zijn er onderwerpen die moeten worden vermeden (bijvoorbeeld ontslagen, gezondheidscrises)?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Dit wordt altijd afgestemd met de opdrachtgever. Dit kan bijvoorbeeld afhankelijk zijn van lopende zaken bij het ministerie of juist niet.

VRAAG 16	Wordt de interactie van gebruikers gemonitord (bijvoorbeeld linkklikken, invoer van inloggegevens, rapporteren van de phishing-e-mail)? Welke specifieke metrics moeten worden verzameld?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Ja, dat is wel gebruikelijk. Dan moet je inderdaad denken aan zaken als muisklikken en, invoering af afgifte van inloggegevens.

VRAAG 17	Moeten gebruikers worden doorgestuurd naar een trainingspagina of bericht na het klikken, of heeft een stille trackingaanpak de voorkeur?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Dit kan verschillen per opdracht. Ervaring leert dat een stille trainingsaanpak niet de voorkeur heeft.

VRAAG 18	Wat is de duur en timing van de campagne (bijvoorbeeld een enkele dag, weken, alleen tijdens kantooruren)?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Dat kan verschillen per opdracht. In het verleden ook campagnes gehad van meerdere jaren.

VRAAG 19	Is deze campagne onderdeel van een terugkerend testprogramma (bijvoorbeeld kwartaalbewustzijnstests) of een eenmalige beoordeling?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Het zal een eenmalige losse uitvraag zijn voor een bepaalde periode.

VRAAG 20	Zijn meertalige phishing-sjablonen vereist op basis van de locaties of taalvoorkeuren van de ontvangers?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Nee

VRAAG 21	Moet de phishingcampagne alleen generieke aanvallen simuleren, of moeten er spear-phishingscenario's worden opgenomen met echte namen, rollen of interne terminologie van medewerkers?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Dit zal afhangen van de uitvraag. Het gaat zeker niet alleen om bulk phishing.

VRAAG 22	Zal de campagne in één golf worden uitgevoerd of in meerdere fasen (bijvoorbeeld om het awarness testen na training)?
Vindplaats	Social Engineering Onderzoeken
Antwoord	Dat kan verschillen per opdracht.

VRAAG 23	Welke systemen of omgevingen vallen binnen de reikwijdte van deze service? Wat is het volume?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dat kan verschillen per opdracht.

VRAAG 24	Zullen we onze eigen hardening-/kwetsbaarheid-/monitoring-/IDS-/IPS-tools gebruiken of beheren, of maken we gebruik van al bestaande tools?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dat hangt wederom van de uitvraag af. Ga er van uit dat je eigen tools gebruikt maar in sommige gevallen is het alleen mogelijk om gebruik te maken van tools die worden aangeboden.

VRAAG 25	Volgen we onze eigen kaders/beveiligingsbaselines/beleid/benchmarks, die van u, of een combinatie daarvan?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Als dit niet wordt gespecifieerd in de opdracht, kunt u die van uzelf volgen.

VRAAG 26	Welke specifieke resultaten of leveringen verwacht je van dit onderzoek?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dit zou gespecificeerd moeten zijn in de opdracht.

VRAAG 27	Zal dit een doorlopende activiteit zijn of op verzoek?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Op verzoek, maar dat kan eenmalig zijn of eventueel over een langere periode of meerdere tests.

VRAAG 28	Zijn er compliance-normen of wettelijke vereisten waarmee we rekening moeten houden tijdens de onderzoeken?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Nee, tenzij opgenomen in een losse opdracht/offerteaanvraag

VRAAG 29	Zijn er beperkingen aan de tijd die we aan de onderzoeken kunnen besteden?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Nee, tenzij opgenomen in een losse opdracht/offerteaanvraag

VRAAG 30	Kun je de soorten softwarekwaliteit en beveiligingsonderzoeken specificeren die je verwacht dat in de opdrachten zijn opgenomen?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dit is afhankelijk van de uitvraag.

VRAAG 31	Zijn er specifieke aandachtsgebieden (bijv. specifieke applicaties, systemen of technologieën) die je als prioriteit beschouwt?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dit is afhankelijk van de uitvraag.

VRAAG 32	Welke specifieke prestatiemetrics of key performance indicators (KPI's) gebruik je om het succes van softwarekwaliteit en beveiligingsonderzoeken te evalueren?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dit is afhankelijk van de uitvraag.

VRAAG 33	Wat zijn je verwachtingen met betrekking tot het rapportageformaat en de frequentie voor de bevindingen van de softwarekwaliteit en beveiligingsonderzoeken?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dit is afhankelijk van de uitvraag. Doorgaans mag een leverancier een eigen rapportage formaat hanteren.

VRAAG 34	Zijn er specifieke sjablonen of standaarden die je verkiest?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dit is afhankelijk van de uitvraag.

VRAAG 35	Hoe zie je de bevindingen van deze onderzoeken geïntegreerd worden in je bestaande systemen of processen?
Vindplaats	Security- en penetratietesten algemeen

Antwoord	Dat is niet relevant voor de opdracht. Het is aan Logius hoe bevindingen worden opgepakt.

VRAAG 36	Zijn er tools of platforms die je momenteel gebruikt waarvan we op de hoogte moeten zijn?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Nee

VRAAG 37	Welke criteria beschouw je als essentieel voor een succesvol softwarekwaliteit en beveiligingsonderzoek?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Criteria die SIG hanteert of ISO 25010. Ook wel eens ASVS gebruikt in het verleden.

VRAAG 38	Hoe beoordeel je de effectiviteit van de uitgevoerde onderzoeken?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dat is moeilijk als je geen harde eisen stelt aan de gehanteerde methodiek. Daar kunnen natuurlijk nog eisen aan worden gesteld bij een individuele uitvraag. Kan best zijn dat we op termijn zoiets vragen als MIAUW (Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde). Dat is bij verlenging van deze toelatingsleidraad niet aan de orde.

VRAAG 39	Wie zijn de belangrijkste belanghebbenden binnen Logius die betrokken zullen zijn bij de beoordeling en goedkeuring van de onderzoeksresultaten?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	De opsteller van de behoeftestelling / uitvraag en betrokken security officier. CISO wordt geïnformeerd.

VRAAG 40	Wat is hun verwachte niveau van betrokkenheid gedurende het proces?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Die zijn direct betrokken bij de security test.

VRAAG 41	Zijn er specifieke industriële beveiligingsnormen of kaders (bijv. OWASP, NIST) waaraan je verwacht dat de onderzoeken zich houden?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	OWASP top tien CWE/Sans top 25 is redelijk gangbaar bij een uitvraag voor een pentest. CIS Benchmarks voor een security review.

VRAAG 42	Hoe zal compliance worden gemeten?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Compliance waarmee? Eventuele bevindingen moeten worden opgelost.

VRAAG 43	Kun je inzichten of voorbeelden geven van eerdere softwarekwaliteit en beveiligingsonderzoeken die onder de DAS zijn uitgevoerd?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Beoordeling van configuratie en hardening van componenten in een VPC / tenant. DigiD assessments Pentesten in alle soorten en maten

VRAAG 44	Welke lessen zijn geleerd die toekomstige onderzoeken kunnen informeren?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Bundelen van uitvragen bijvoorbeeld binnen een Agile Release Train. Dat is minder werk voor de uitvragen en aanbieder.

VRAAG 45	Hoe zie je ons team samenwerken met jouw interne IT- of ontwikkelingsteams tijdens de onderzoeken?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Coördinatie verloopt doorgaans via de Security officer van de trein of voorziening.

VRAAG 46	Zijn er specifieke processen of protocollen die we moeten volgen?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Anders dan wordt gevraagd tijdens een specifieke uitvraag, nee.

VRAAG 47	Welke risicobeheerstrategieën heb je momenteel in place met betrekking tot softwarekwaliteit en beveiliging?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Dat hangt van de voorziening af, maar bij puur technische maatregelen kun je denken aan: SAST DAST Dependency scanning Secret scanning Scanning op kwetsbaarheden van images en VMs. Scanning op naleving van hardeningsrichtlijnen Scanning op toepassing van internetstandaarden

VRAAG 48	Hoe verwacht je dat onze onderzoeken aansluiten bij deze strategieën?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Kan worden gezien als een extra controle van een derde partij. Informatiebeveiliging zou in principe op orde moeten zijn. Kan ook sprake zijn van een migratie of grote wijzigingen in een voorziening die een handmatige security test noodzakelijk maakt.

VRAAG 49	Welke feedbackmechanismen heb je in place om de kwaliteit van ons werk aan softwarekwaliteit en beveiligingsonderzoeken te beoordelen?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Zie Vraag 38. Hangt ook af van de prettige samenwerking en bevindingen.

VRAAG 50	Hoe zal deze feedback worden gecommuniceerd?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Doorgaans mondeling. Het is ongewoon om naast een kick-off ook een afsluitend gesprek te voeren

VRAAG 51	Naarmate het technologie-landschap evolueert, welke toekomstige behoeften of uitdagingen voorzie je die de reikwijdte van softwarekwaliteit en beveiligingsonderzoeken kunnen beïnvloeden?
Vindplaats	Security- en penetratietesten algemeen
Antwoord	Moeilijk te zeggen. Dat zal de toekomst uitwijzen. Ik verwacht meer gebruik van AI bij security tests.